Good Practice in Action 105
Legal Resource

The General Data Protection Regulation (GDPR) legal principles and practice notes for the counselling professions

bacp | counselling changes lives

Good Practice in Action 105
Legal Resource

T: 01455 883300 **F:** 01455 550243
E: bacp@bacp.co.uk **www.bacp.co.uk**

Design by Steers McGillan Eves.

Updated January 2019

Contents

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*, the UK data protection legislation including the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) in respect of the law regarding data protection in England and Wales. In Scotland and Northern Ireland, practices and legal provisions may be different, and further publications specific to these areas may follow. Meanwhile references to sources of information are included to assist members working in these jurisdictions.

Using the legal resources

BACP's *Ethical Framework* (BACP 2018) requires members to 'keep accurate records that are adequate, relevant and limited to what is necessary for the type of service being provided', and to 'comply with the applicable data protection requirements' (BACP 2018: Good Practice 15). https://www.bacp.co.uk/news/news-from-bacp/2018/16-april-2018-ethical-framework-review/

These legal resources are intended to support good practice by offering general information on legal 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 legal resource were up to date at the time of writing but there may be changes to the law, government departments, websites and web addresses.

In this resource, 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.

Back to contents

Introduction

What this legal resource provides

The law relating to data protection is complicated because it comprises several pieces of legislation, all of which need to be read and implemented together. The law is in the process of development in the UK at the moment, and will evolve more over time, so it is important for practitioners to keep up to date with any changes. Updates are available on the website of the Information Commissioner at www.ico.org.uk.

As this is such a huge area of law, this resource provides a brief outline of the relevant provisions. If practitioners are in any doubt about the data protection law or its application to their practice, there is more detailed information on the website of the Information Commissioner at www.ico.org.uk, and there is a helpline on that website for small businesses.

Note: although some parts of the data protection law are referenced here, these are not exclusive, and reference should be made to the data protection law in its entirety. Data protection law is currently still developing, and the Information Commissioner's website will have up to date information and guidance as the new law unfolds. The Information Commissioner's Office (ICO) will offer guidance on specific issues and respond to enquiries.

This resource should help you to identify and understand:

- situations where data protection legislation applies
- the main provisions of the *General Data Protection Regulation* (GDPR)
- the law relating to consent in the context of data protection
- the specific principles of the data protection legislation applicable to vulnerable adults and children
- the data protection law in the context of research

and how to:

- manage confidentiality in the context of data protection legislation
- document and record data protection compliance in a way that meets the requirements of the law

Back to contents

- identify situations where legal or other professional advice should be sought in relation to data protection and information sharing and which advice would be appropriate

- make decisions concerning data protection which are within the law and comply with BACP's *Ethical Framework for the Counselling Professions* (BACP 2018).

The General Data Protection Regulation (GDPR)

By now, most of us will be familiar with the general principles of the General Data Protection Regulation (GDPR). This is a General Regulation that was passed by the European Parliament and the Council of the European Union, and is binding on all members of the European Union. It came into force for the UK and all member states on 25 May 2018. As a Regulation it has 'direct effect' so it is not dependent on enabling legislation by the Member States.

The GDPR gives power to each of the member states to make their own rules for the practical implementation of the GDPR in their country and the DPA includes provisions about how the GDPR applies in the UK. However, the provisions of the DPA are not limited to the GDPR, it also contains additional law applicable to the UK (for example, relating to immigration, national security, etc.).

The Data Protection Act 1998, with which we have been familiar, has been repealed in its entirety, and replaced by the GDPR and the Data Protection Act 2018 (DPA).

After the UK's exit from the EU (Brexit), the European Union (Withdrawal) Bill 2017-2019 as currently drafted will transpose EU laws (including the GDPR) into UK law on "exit day", which is currently 11pm on 29 March 2019. The UK Government and the EU are also negotiating a withdrawal agreement which is anticipated to provide for a "transition period" from 30 March 2019 to 31 December 2020 during which the UK will continue to be subject to EU law on the protection of personal data.

Back to contents

1. When does data protection legislation apply?

- Personal data can only be processed on one of the six lawful bases in the GDPR (Art 6)
- consent of the data subject to process for one or more specific purposes
- processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- processing is necessary for compliance with a legal obligation to which the controller is subject
- processing is necessary to protect vital interests of the data subject or of another natural person
- processing is necessary for performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- processing is necessary for legitimate interests of controller or a third party, except where those interests are overridden by the rights and freedoms of the data subject.

Practitioners in counselling and psychotherapy professions who are members of the BACP are required under the BACP's *Ethical Framework* to:

> *keep accurate records that are adequate, relevant and limited to what is necessary for the type of service being provided and comply with the applicable data protection requirements.* (BACP 2018: Good Practice, point 15)

We are also required to provide our clients with the relevant information and enter into an agreement or contract with them about the terms on which our service will be provided (BACP 2018: Good Practice, points 30–31).

Many details of how GDPR is applied are still unclear. Full clarity will only gradually appear over the next few years as more guidance is produced and case law defines the precise contours of the legislation. BACP's *Ethical Framework* (BACP 2018), like the GDPR is based on openness and transparency, so that even if you are not yet completely clear about how to interpret the provisions of the GDPR, it is helpful to be absolutely transparent with clients (who are your data subjects) at all stages of the counselling relationship.

Back to contents

The 'Lawful basis' defined in the GDPR underpinning our work with clients

The GDPR insists that we cannot hold or process anybody's personal data unless there is a 'lawful basis' for doing so.

In addition, if we process sensitive data we will need an additional lawful basis for this.

1. Lawful basis for processing data

In the counselling professions, we are usually providing a service to clients on the basis of a contract with them or (in the case of children who are not competent to make a contract), with those with parental responsibility for them.

Counsellors working in the NHS healthcare services may be doing so in the context of that service. Other counsellors may work in the context of social care, adoption services, schools counselling, etc. Therefore the lawful basis on which we work may vary with the circumstances in which the service is provided.

There are six lawful bases:

- consent;
- contract;
- legal obligation;
- vital interests;
- public task; and
- legitimate interest.

and no basis is 'better' or more important than the others. We must determine our lawful basis before we begin processing data.

It is important to get our bases right first time as the ICO has made it clear that we should not swap to a different lawful basis at a later date 'without good reason' and in particular that if we choose 'consent' we cannot 'usually' swap to a different basis.

If our therapy working environment and/or professional practice require us to keep appropriate records of our work (see the *Ethical Framework* BACP 2018), and records are therefore necessary for our service, then our lawful basis for processing data under the GDPR is likely to be 'necessary for the performance of a contract'.

Back to contents

Another possible basis may be 'legitimate interest' when we are providing services without a client contract, for example in the context of providing NHS healthcare or social care services.

'Consent' has a special meaning under the GDPR in the case of lawful basis, which is different from the colloquial counselling meaning (e.g. where a client gives their consent for therapy), and so where the keeping of records is a condition of receiving therapy, 'consent' is not always the obvious choice for a lawful basis – the ICO states "If you require someone to agree to processing as a condition of service, consent is unlikely to be the most appropriate lawful basis for processing."

So – the two most likely bases for processing a client's personal data, which are available to a BACP member, will usually be 'contract' or, in cases where there is no contract, 'legitimate interest'. There may be other circumstances where 'consent' may be appropriate. If in any doubt, seek legal advice on this issue, or consult the ICO small business advisors, through the ICO website.

2. Lawful basis for processing special category (sensitive) data

If we are processing special category data, we are further required to identify a special category condition for processing and to document this.

The basis for *processing special category* data will usually be 'for the provision of health or social care or treatment' though consent may in some instances be more appropriate here.

Practice Note

If a client is giving explicit consent to the processing of their data, the basis on which data will be gathered, stored, disclosed and destroyed should be clearly set out in your Privacy Notice, separated from the other terms in the therapy contract (such as modality, session length, fees etc.) and the privacy/confidentiality notice consent form should be signed separately from the therapy contract.

Other lawful bases listed above may also apply to certain aspects of our work. If practitioners wish to check the lawful bases, the ICO has provided an online interactive guidance tool at https://ico.org.uk/for-organisations/resources-and-support/lawful-basis-interactive-guidance-tool.

Back to contents

The data protection legislation applies to 'controllers' and/or 'processors' (see 1.2 for definitions) who process personal data concerning 'natural persons' (i.e. human beings and not legal persons such as companies) by 'automated means' or through a manual, structured 'filing system'.

Most controllers must pay an annual fee to the ICO, where personal data are processed by 'automated means'. Controllers may in some circumstances be exempt from paying a fee (see Part 14).

This law applies to all controllers and processors, irrespective of whether or not a fee is payable.

To check whether the data protection legislation applies to you or your organisation, see 1.1 and 1.2, and to check if you have to pay a fee, see Part 14.

1.1 Processing data by 'automated means' and 'filing systems'

Practice Note

The *Ethical Framework* requires BACP members to keep records appropriate to the type of therapy work undertaken, and to comply with data protection requirements, see (BACP 2018: Good Practice, point 15). Records may be kept in a form appropriate to the needs of the service provided, the practitioner, and the client.

The GDPR refers to 'automated means' of data processing including computers, and other forms of automated data processing, retrieval and storage. The ICO guidance, *The Data Protection Fee. A Guide for Controllers* (2018a) defines computers as: 'any type of computer, for example cloud computing, desktop, laptop, tablet'. It also includes other types of equipment which, although not normally described as computers, nevertheless have some ability to process automatically. Examples include 'automatic retrieval systems for audio and visual systems, electronic flexi-time systems, telephone logging equipment, CCTV systems and smartphones'. For fees, see Part 14, and the Glossary.

Back to contents

A 'filing system' in terms of the data protection legislation, means any filing system which is logically ordered so that items can be found by reference to certain specified criteria, for example, this may include filing systems that contain:

- all the information about a client in one file
- client name and contact details in one place, with a link to the client's records in a different place
- client information filed in any other logical or according to clear criteria, (such that a 'temp' working in the practitioner's office could find their way round the filing system).

Practice Note

All practitioners who keep paper client records are strongly recommended to keep them as a logical and orderly filing system for ease of use and to deliver the best possible service. This will be a 'filing system' that falls within the GDPR definition, and therefore the data protection legislation will apply to them.

See GDPR Art 4 (6):

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. In the *Ethical Framework* we are committed to keeping records as follows:

We will keep accurate records that:

- *are adequate, relevant and limited to what is necessary for the type of service being provided*
- *comply with the applicable data protection requirements – see www.ico.org.uk.* (BACP 2018, Good Practice, point 15)

Note: There is therefore a strong legal and ethical expectation that appropriate records will be kept. Practitioners have been criticised in court and in complaints proceedings for failing to keep appropriate and adequate records.

Back to contents

The term 'records' is defined in the 'Glossary' to the *Ethical Framework*:

> **Record**
>
> *A catch-all word that includes all notes, records, memoranda, appointments, communications and correspondence, photographs, artefacts, video or audio recordings about an identifiable client. Records may exist in any format, typically but not exclusively, on paper or electronically. There is no distinction between factual and process notes in what the law regards as a record* – (BACP 2018: C2e, Good Practice, points 15, 31d, 31e, 71)

In some rare situations, and very exceptionally practitioners may consciously and deliberately decide to provide services to clients without keeping any form of records if:

- the circumstances prevent making and keeping any records securely and adequately protected from misuse or intrusion by others
- clients refuse to provide the consent necessary to permit the keeping of records and the practitioner is willing to provide a service on this basis, and/or is permitted to do so by agency policy
- keeping records is deemed to be unnecessary for the type of service being provided. For example, a community-based service in which clients drop in on an informal basis without prior appointment or any expectation of an ongoing service or if there is a public good being served by the provision of a service and clients would be deterred by the existence of records. Good practice in these circumstances requires that the absence of any records is the outcome of a deliberate policy decision and communicated to clients and any service stakeholders.

Note: Practitioners who decide not to keep any records should be aware that the absence of any records will make resolving any disagreements with clients about what has occurred much harder to resolve and may leave the practitioner unable to successfully defend themselves in any professional conduct proceedings or to provide supported and reliable evidence in any court proceedings related to their therapy practice. Advice from lawyers and insurers consistently supports keeping records.

Back to contents

1.2 To whom does data protection legislation apply?

Practice Note

The provision of counselling and psychotherapy, or any form of counselling related services is regarded by the law as a business. If we process any personal data concerning a 'natural person' by 'automated means' (for example, a computer, laptop, smartphone etc.), or if we run a structured 'filing system', the data protection laws are likely to apply to us and to our business – for more on this and definitions, see Part 1.1 and the Glossary.

To check if the legislation applies to you, see the ICO's Data *Protection Self-Assessment Toolkit* at https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/.

Our personal responsibilities as practitioners will depend on our own role as 'controller' and/or 'processor' of the personal data and the way in which the data and filing systems in our business are managed. If we are self-employed (for example, practising as sole traders), or work in partnerships or for larger organisations then those roles may be different. See Table 1A to ascertain which role might be applicable to your therapy business. As will be seen from the table, we can sometimes hold both the role of 'controller' and 'processor', especially if we work alone or in a small organisation.

In addition, it should be noted that we do handle special categories of personal data (see definitions below) and these are the most sensitive data from a compliance perspective with additional obligations.

One additional fundamental obligation the GDPR has introduced is that of accountability and the need to demonstrate compliance (see Part 3).

It is essential for counsellors and psychotherapists to understand the concept of a *data controller* and a *data processor*. The Information Commissioner's Office (ICO) explains that the data controller exercises '*overall control over the purpose for which and the manner in which personal data are processed.*' A processor on the other hand is '*any person (other than an employee of the data controller) who processes the data on behalf of the data controller'.*

In practice this means that the majority of counsellors and psychotherapists in private practice are likely to be data controllers. A controller can be an individual or an organisation, this depends largely on the legal entity through which we practise.

Questions for reflection:

- Do I practise on my own and have not set up a company and are not employed by a formal legal structure such as a company or partnership? If so, then individually I will be the controller.

- Have I have set up a company or work with a group of counsellors in a company or partnership? If so, then the controller will be the organisation.

An organisation which is a legal entity must, under the GDPR, contractually bind its processors (including contractors, outsourced service providers, or volunteers) to participate in processing personal data in accordance with the GDPR and assisting in fulfilling the organisation's role of controller.

If a counsellor is an employee of a data controller (such as a school, university or a counselling service) they will also be a controller, with responsibilities which will be in proportion to their role and seniority in the organisation. The employer should be registered with the ICO, and the counsellor's contract should set out the way in which they are expected to deal with the gathering, storage and protection of personal data in the counselling records.

Some practitioners may wear a 'controller' or a 'processor' hat in different situations. For example, they may be a controller in their own private practice and as an employee or as part of a partnership. If they operate as a freelance contractor they will either be a joint controller or a processor, depending on their contract.

For practitioners working independently as freelance contractors to an organisation, for example, those providing employee counselling services (EAPs), the distinction between being an independent contractor and being an employee is important, for tax and for GDPR reasons, so it is important to examine carefully any applicable contract to see what it says about employee status, data protection, and who holds responsibility for the counselling records. If uncertain, it is wise to seek legal advice, which may be available free from your professional insurer, and information is available from HMRC at https://www.gov.uk/employment-status/selfemployed-contractor.

Back to contents

Data controllers (assuming that they use some form of electronic devices to manage their client's personal data) will need to pay a fee to the Information Commissioner's Office. This can be done online at https://www.gov.uk/data-protection-register-notify-ico-personal-data.

Practitioners running a small company will hold the responsibility to ensure that any staff they employ understand their responsibilities under the GDPR – and if they contract any other companies to provide services (for instance, if they operate out of a shared office building where reception is provided by the landlord), they will need a data processor agreement with any contractors that handle any client personal data.

More about GDPR for small businesses is available at https://ico.org.uk/for-organisations/business/.

Definitions: The roles of 'controller' and 'processor' are defined in the data protection legislation and subject to specific rules.

'Controller' is defined in the GDPR Art 4 (7) as:

> *(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*

'Processor' is defined in the GDPR Art 4 (8) as:

> *(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

Practice Note

Examples:

A therapist working as a sole trader, at home, or in a rented room, may be both a controller (for example, when processing their own clients' personal data) and a processor (if, for example, the therapist is engaged by another organisation as a self-employed contractor).

Back to contents

An organisation or agency, which makes the decisions about the purpose and means of processing the personal data of its clients and personnel, is likely to be a controller. Note that therapists who are employed by that organisation or agency, or who are working as volunteers for that agency, will be fulfilling the controller's tasks and will not be considered to be third-party processors.

The data protection legislation creates rules regulating the 'processing' of 'personal data' and includes 'special categories' as follows:

'Personal Data' are defined in the GDPR Art 4 (1) as:

> *(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

'Special Categories of Personal Data' in GDPR Art 9 (1) are defined as:

> *(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, physical or mental health condition, any offence the data subject has actually or allegedly committed or any proceeding relating to the alleged offence and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*

The GDPR (35) provides additional context to the above definition and construes the subject very broadly and includes information concerning the data subject's past, present and future health; any identifiers used by a health care provider; examination and test results; samples; diseases, disabilities, disease risk and medical history. The GDPR has now added genetic and biometric data to the existing legislation and Member States may introduce further conditions relating to genetic or biometric data or data concerning health.

The processing of 'Special Categories of Personal Data' as defined in the (GDPR: Art 9 (1)) is prohibited unless the exceptions in (GDPR: Art 9 (2)) apply. The highest penalties can be imposed for breaches of Article 9.

Back to contents

Exceptions listed in (GDPR Art 9 (2))

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where pro*hibited by Union or Member State law;*

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

Back to contents

> *(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety* of health care *and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or*
>
> *(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. (GDPR: Art 9 (1))*

The special categories of data defined in (GDPR: Art 9 (1)) may be processed for the purposes set out in (GDPR: Art 9 (2h)), if the processing is carried out by a professional, who is subject to an obligation of professional secrecy.

'Processing' is defined in the GDPR Art 4 (2) as:

> *(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.* (GDPR Art 4 (2))

Checklist: How might the terms 'controller' and 'processor' apply to me and/or my therapy practice?

Q 1 Do I personally:

- collect, record,
- organise, store,
- adapt or alter,
- retrieve, consult or use,
- disclose by transmission,
- restrict, erase or destroy any personal data?

Answered 'Yes' to any of these? *You are processing personal data and the data protection legislation will apply to you.*

Please go on to Q 2.

Back to contents

Q 2 Am I in therapy practice as a sole trader or running my own business?

Answered 'Yes' to this? *You are likely to be a controller in relation to the parts of the practice where you have power to determine the purpose and means of the data processing.*

Please note that therapists may have a mixed practice, and so may be both a controller and a processor in different aspects of your work. As an example, you may have a mixed therapy practice comprising part private work (i.e. self-employed practitioner as a sole trader etc.) and part employment or voluntary work for an organisation, agency, etc. You may also be a processor of data (for example, if engaged by another organisation as a self-employed consultant). Additional provisions of the GDPR will apply to you and to your contractual relationship with the data controller.

Please go on to Q 3.

Q 3 Is my therapy practice wholly (or partly) owned or run by someone else, (i.e. a company, public authority, agency or other legal person)?

Answered 'Yes' to this? *The legal person, authority, agency etc. who owns or runs all or part of your practice is likely to be the controller. If you are employed by, or volunteer with, the practice you will be processing personal data as part of the data controller organisation. Additional provisions of the GDPR will apply to the data controller and also to their contractual relationship with you.*

Back to contents

2. When does data protection legislation NOT apply?

2.1 Personal or household activities

Data protection and the GDPR does not apply to processing data by a 'natural person' (i.e. a human person and not a legal entity such as a company, partnership, local authority, organisation, agency, etc.) in the course of personal or household activities such as keeping personal diaries, personal and family phone contacts, or storing papers such as household bills etc. *The key is that there must be no connection to a professional or commercial activity.*

> *This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities. (GDPR: (18))*

2.2 Personal data concerning 'legal persons' (i.e. not 'natural persons')

The GDPR is designed to protect the processing of personal data concerning 'natural persons' (i.e. human beings and not legal entities) (GDPR Art 1 (1)). If the data which are processed solely concern a 'legal person', i.e. a company, legal business partnership, organisation, etc., the data protection legislation will not apply.

> *The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person. (GDPR: (14))*

2.3 Personal data processed by a competent authority in relation to criminal offences or public security

If personal data are processed by a competent authority (e.g. police, the courts, probation and prison services etc.) and solely relate to the following then the GDPR will not apply:

...purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data... See GDPR (19) for more information.

Instead, this is covered by the Law Enforcement Directive ((EU) 2016/680) and the DPA.

2.4 Personal data processed manually and also not in a structured 'filing system'

If personal data are processed manually, and not by any form of automated means, and also not processed in any form of structured 'filing system', as defined in the GDPR, then the GDPR will not apply. For these definitions see the Glossary, and for explanations see Parts 1.1, 1.2, and Table 1A.

Practice Note

However, please note that many, if not most practitioners will keep their records:

- on a computer or laptop, and/or
- upload records to a web-based storage system or database, and/or
- keep records manually in a logical and structured filing system.
- many of us will also use some sort of automated processing of client data, for example, contacting clients using smartphones, message systems, emails, etc.

If personal data are processed in any of these ways, then the GDPR applies.

Back to contents

2.5 Completely anonymised data are not subject to the GDPR

See the Glossary for definitions of anonymisation and anonymised, and the contrast with pseudonymisation of data which makes data subject to GDPR. Anonymised information ceases to be 'personal data' with the associated legal requirements and protection when any means of identifying the person concerned has been genuinely and irreversibly removed. The GDPR is very clear:

> *The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person, or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This regulation does not therefore concern the processing of anonymous information, including for statistical or research purposes. (GDPR (26))*

Practice Note

As a practitioner it is safest to assume that GDPR does apply and that the exceptions will rarely, if ever, apply.

3. The GDPR applies to me/ my therapy practice – what must I do now?

See Part 1 and the checklist to decide whether the GDPR and/ or the DPA apply to you and/or your practice. If so, then the next issue is to decide:

Q1 Am I a controller or a processor, or both?

The checklist will also help to clarify whether you are a 'controller', a 'processor', or you may hold both roles. The requirements placed on practitioners will be different for these roles, with more responsibilities placed on controllers.

Q2 Fees: Are controllers liable to pay an annual fee to the ICO?

Therapy is a business for tax and for data protection purposes, irrespective of whether it is one person working as a sole trader, or a large organisation. There are different levels of fee, depending on the size of the organisation involved. Many therapists will fall into the category of 'Tier 1 "micro-organisations"', that is, those with a maximum turnover of £632,000 for the financial year or no more than 10 members of staff. The current fee for Tier 1 is £40, with a £5 discount for direct debit payments. See Part 14 for more about the fees payable, and the exemptions that apply.

Parts 4–11, and Part 13 look at the main general provisions of the GDPR, in relation to the respective responsibilities of controllers and processors.

Back to contents

4. Specific provisions of the GDPR for 'controllers'

4.1 Demonstrating that processing is in accordance with the regulation

A controller has the responsibility to:

- demonstrate compliance with the GDPR, through policies where appropriate, or creating codes of conduct (GDPR Art 25 (1))
- put in place the necessary technical and organisational measures to ensure compliance with the GDPR (GDPR Art 25 (1))
- ensure that personal data in records are limited to those which are necessary for the specific purpose. This includes collection, processing, storage, and accessibility (GDPR Art 25 (2))
- enter into a written contract with processor(s) stating the purpose, terms and means of processing personal data on behalf of the controller (see Part 5.1).

There may be joint controllers sharing these obligations. Controllers should only use processors who can implement the necessary technical measures to fulfil their duties under the GDPR (GDPR Art 28 (1)). The contract between the controller and the processor should clearly state the processor's responsibilities under the GDPR (GDPR Art 28 (3)). For these responsibilities, see Parts 5 and 13. For the terms of the written contract see Part 5.1.

4.2 Controller's records of processing activities

Under (GDPR Art 30 (1), (4)) controllers must maintain a record of processing activities in a written or electronic form, stating the processing activities carried out on behalf of the controller, under their responsibility:

That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and... the documentation of appropriate safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). (GDPR Art 30)

Article 32 refers to security measures in processing, for more on this, please see Part 6.

There is a limited exemption for small and medium-sized organisations (see section 13 below).

4.3 Controller's duty to notify personal data breach to the supervisory authority (ICO) and to the data subject

Under the GDPR (Art 33 (1)), if there is a breach of personal data, the controller must, 'without undue delay, and where feasible, within 72 hours after having become aware of it', notify the breach to the supervisory authority (in the UK this will be the ICO); unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification is not made within 72 hours, reasons must be given for the delay.

'The notification should at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. (GDPR Art 33 (3))

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article. (GDPR Art 33 (4–5))

Notifying the data subject of a data breach

There is an obligation under the GDPR (Art 34) for the controller to notify the data subject of any personal data breach which is likely to result in a high risk to the rights and freedoms of natural persons, and to include the information at (GDPR Art 33 (3) (a), (b) and (c)) listed above. If this is not done as required, the ICO may either order them to do so, or consider that an exemption applies. There are some exemptions to the requirement to notify:

Notification to the data subject is not required if:

(a) the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

5. Overview of the main provisions of the GDPR relevant to 'processors'

5.1 Contract between the controller and the processor

There must be a legally binding contract (or other binding legal act) in writing between a controller and each of the processor(s) who work on the controller's behalf (GDPR Art 28 (3)).

The terms of the contract (or other binding legal act) should include:

- subject matter and duration of the processing
- the nature and purpose of the processing
- type of personal data
- categories of data subjects
- obligations and rights of the controller.

In particular the contract (or other binding legal act) shall stipulate that the processor will guarantee to:

- only process personal data on the documented instructions of the controller (with some exceptions where the law or important public interest requires disclosure (GDPR Art 28 (3a))
- ensure that personnel authorised to process the personal data make a commitment to confidentiality, or are under a statutory obligation to confidentiality
- take all required measures to secure personal data
- respect the conditions for engaging another processor (a 'sub-processor' – see Part 5.2)
- assist the controller in fulfilling the rights of the data subject (see Part 6)
- assist the controller to comply with security by taking into account the nature of the processing and information available to the processor

Back to contents

- at the choice of the controller, delete or return all the personal data to the controller at the end of the provision of services relating to the processing, and delete existing copies unless the EU law requires storage of the data

- provide information to the controller and allow audit and inspections as required under the GDPR.

5.2 Contract between the processor and another processor

The GDPR is strict about the engagement of a processor by another processor (a 'sub-processor'):

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. (GDPR Art 28 (2))

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor ...shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations. (GDPR Art 28 (4))

This is quite an onerous requirement, as it means that if a practitioner who is a processor of client records engages a sub-processor (for example, Google Cloud or another cloud service provider):

- the controller must have authorised the engagement of the other processor;

- there be a written contract between the two processors reflecting all the GDPR requirements, (see Part 5.1); and

- the practitioner remains liable for the sub-processor's compliance with data protection law.

Practice Note

Adherence by both the controller and the processor(s) to a Code of Conduct created by a body representing the sector and approved by the ICO, and/or an approved certification mechanism might be used to demonstrate sufficient guarantees of compliance with the requirements of the GDPR. However, the ICO has no plans to accredit certification bodies or to carry out certification at this stage.

5.3 Responsibility of processors

The ICO website (www.ico.org.uk) summarises these as:

'A processor must only act on the documented instructions of a controller. If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

In addition to its contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:

- *not to use a sub-processor without the prior written authorisation of the controller;*
- *to co-operate with supervisory authorities (such as the ICO);*
- *to ensure the security of its processing;*
- *to keep records of processing activities;*
- *to notify any personal data breaches to the controller;*
- *to employ a data protection officer; and*
- *to appoint (in writing) a representative within the European Union if needed.*

If a processor fails to meet any of these obligations or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.' See also the (GDPR Art 28).

Back to contents

5.4 Processor's records of processing activities

Under the GDPR, the processor and any representative of the processor, shall maintain a written or electronic form record of the processing activities carried out on behalf of the controller, including:

> *2 (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;*
>
> *(b) the categories of processing carried out on behalf of each controller;*
>
> *(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;*
>
> *(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). (GDPR Art 30 (2))*

The processor must notify the controller of any security breach (GDPR Art 33 (2)). For security measures, see Part 6.

The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

See Part 13 for documentation of compliance with the GDPR.

6. Security measures in processing

Security measures to protect personal data can take into account the costs of implementation, and the nature, scope, purposes and context of the processing, as well as the varying likelihood and severity of risks to the freedoms of the natural persons to be protected.

Recognising data breaches and logging them into a data breach log are essential. Just like an accident book, the data breach log should record all breaches, however minor. That way, if there is a major breach and the ICO does an audit, they will be encouraged to see that we have taken our breach log seriously.

6.1 What is a data breach?

The ICO defines a personal data breach as, '...a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.' see ICO; 2018. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

So, for example, if a computer or paper client record is damaged by flood (or spilled coffee!), that could constitute a significant data breach. The most common cause of a data breach is poor email practice. For instance, putting email addresses into the 'cc' field rather than 'bcc', or leaving a long email trail with sensitive earlier email correspondence included below the current message.

Paper files are just as open to data breaches...leaving a client diary with sensitive data or client notes out in a shared room, or on a café table, leaving a printout in the office printer tray for others to see, not adhering to a strict clear desk policy and failing to lock the computer screen when someone else could see personal data, could all result in data breaches which will need to be logged... see 6.2.

Back to contents

6.2 What should we do if there is a data breach?

If you are a processor, you must notify the controller of any data security breach (GDPR Art 33 (2)). Controllers have a duty to maintain a log of their activities, usually referred to as a 'data breach log' or 'data breach file'.

All data breaches should be logged in a 'data breach file'. However, minor breaches may not necessarily need to be reported to the ICO, provided that the controller has identified any possible risk to the client arising from the breach and that any potential risk has been dealt with appropriately, so that there is no adverse impact on the client.

The ICO states: 'When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then you must notify the ICO; if it's unlikely, then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it. ...This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors... So, on becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.' ICO; 2018. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

In the spirit of transparency and openness in our work, the *Ethical Framework* (BACP 2018) requires that we are open with our clients about any breach of confidentiality and that we do our best to minimise any risk to clients or others arising from our actions.

The GDPR expects the same ethos of transparency, but the ICO may not necessarily want to be overwhelmed by reports of minor breaches which have been dealt with and where there is no risk to the client.

If there is any risk to the client, then a report must be made, and you may also need to inform other parties such as your insurance provider. Where there is any doubt about whether to report a breach, see the ICO website and seek legal or other appropriate advice, for instance from the ICO helpline (https://ico.org.uk/global/contact-us/helpline/).

For security measures, see 6.3

6.3 How we might protect the security of our data

One of the principles of the GDPR is that the data controller (and any processors) have an obligation to keep data safe. The level of data security required is directly related to the sensitivity and quantity of data.

There is insufficient space here to explain in detail how to implement data security, so it is helpful to get advice from a trusted local IT service. It would be helpful to put some or all of these basic measures in place, as appropriate to the service provided:

Security measures may include:

a*) the pseudonymisation and encryption of personal data; [see Glossary]*

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (GDPR Art 32 (1a–d))

e) Finding out how to encrypt your computers, tablets and phones, and so protect client data, and also safeguard your personal data

f) Password protecting email attachments. If you are sending any personal information by email, it is best to put it into a file and then you can password protect the file. If you use a version of Microsoft Office, you can find information on how to do this at https://support.office.com/en-us/article/add-or-remove-protection-in-your-document-workbook-or-presentation-05084cc3-300d-4c1a-8416-38d3e37d6826. Remember that, for best protection, if you have emailed a password-protected document, you should then send the password by another means, such as by text, and not to the same email address.

g) Finding out how to obtain and use two-factor authentication wherever possible. This is a service that is increasingly available for many online services such as email and cloud hosting. It means that your password alone does not provide access to the service; they typically send a code to your mobile phone that you also need to enter. This is particularly important for your email account, but it would also apply to your Dropbox or other online file storage service.

h) Keeping all your software updated. The operating system of your PC or phone should be updated as regularly as possible to ensure any faults or weaknesses that have been identified are patched (repaired).

Back to contents

i) Using a high quality anti-virus and internet security package.

It is helpful to have a separate email account for counselling work, which is supplied by an email service that is secure and encrypted by default. A trusted IT advisor can help to identify these.

j) Using a privacy screen on your smartphone so that people cannot easily see any information over your shoulder in shared or public spaces.

k) There are a number of security measures that apply to paper records, such as:

i. Secure shredding or destruction of all paper containing personal data

ii. Use of a robust, lockable filing cabinet

iii. Where personal data are printed out, retain them as part of the client record only for so long as is necessary for the therapy work and as agreed with the client in the therapy contract

iv. If you wish to keep a 'back-up' copy of client data, keep the copies in separate places, then if one set of data is destroyed, the other may be safe. However, if you hold identical client data on computer and on paper, be aware of the protection required for both forms of data storage.

v. Protect documents from others' view and maintain a strict 'clear desk' policy. If you work in shared premises or rooms, or work from home, do not leave the computer, tablet, or phone on when leaving the room, allowing others to view any unencrypted client data, emails or files.

The ICO's guidance on data security is at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/ (accessed 5 Jan 2019). The Government cyber security portal is at: https://www.gov.uk/government/cyber-security.

Other relevant GDPR provisions in Article 32 include:

In assessing *the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. (GDPR Art 32 (2))*

3 Adherence to an approved code of conduct ...may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. (GDPR Art 32 (3))

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller unless he or she is required to do so by Union or Member State law. (GDPR Art 32 (4))

7. The rights of the data subject

7.1 The right to be informed

The controller must communicate to the data subject the rights they have with regard to the processing of their data:

> *in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.* (GDPR Art 12 (1))

This information must be provided at the time the controller collects the data subject's personal data.

The GDPR (Art 13) sets out a list of certain information that data subjects have a right to be told. This includes:

> *(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;*
>
> *(b) the contact details of the data protection officer, where applicable;*
>
> *(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
>
> *(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*
>
> *(e) the recipients or categories of recipients of the personal data, if any;*
>
> *(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission… or …reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. (GDPR Art 13 (1))*
>
> *2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:*

Back to contents

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, … and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any other purpose and with any relevant further information as referred to in paragraph 2. (GDPR Art 13 (2–3))

7.2 Informing the data subject of their rights, when personal data are not collected from the data subject

This situation could occur where information is gathered from an external source accessed by the controller or processor. Where personal data are collected, but not from the data subject, the data subject (who may have been totally unaware that data was collected) needs to know that their data are being collected and processed, and of their rights. GDPR (Art 14) sets out the rights of the data subject in this situation. The list is similarly worded to that set out in Article 13 (see Part 7.1 above), but the controller must also inform the data subject of the categories of personal data concerned, and the source from which the personal data originate, and whether they came from publicly accessible sources.

Back to contents

This information must be provided to the data subject within a reasonable period of the controller obtaining the data and no later than one month.

Table 7A: Summary of the specific rights of a data subject

Under GDPR (Art 14), the controller must provide the data subject with the following information about their rights under the GDPR necessary to ensure fair and transparent processing in respect of their data.

These rights include:

- to know how long their data will be stored, or the criteria for deciding this; and also
- any legitimate interest in the data pursued by the controller or a third party.

The data subject also has the right to request from the controller:

- access to their personal data
- rectification of personal data
- erasure of personal data
- restriction of processing concerning the data subject

and also the right to:

- object to processing as well as the right to data portability
- withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- request information about the existence of automated decision-making, including profiling.

These rights are explored in more detail in Parts 7.3.1–7.3.7.

Note: All these rights exist on the proviso that they will not affect the rights and freedoms of others, and that they cannot be exercised in contravention of a court order, or the public interest.

Practice Note

In the context of personal data gathered in the counselling professions, rights of the data subject can usually be addressed in negotiating the initial contract between the client and the practitioner.

The client should also be made aware of:

- the circle of confidentiality of the records, (see Glossary)
- limitations on confidentiality (see Part 9), and
- the period for which the records will be stored.

7.3 Specific rights of the data subject

The controller must facilitate the exercise of the data subject's rights unless they cannot identify the data subject (GDPR Art 12(2)). This is the reason for the identity of the data subject being proven (if possible)

7.3.1 Access to personal data

Information to be provided

The GDPR at Article 15 provides for the right of the data subject to obtain from the controller confirmation that personal data are being processed about them, and the right of access to that personal data. The rationale for this is explained:

> *(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. (GDPR (63))*
>
> *Under Article 15, the data subject is entitled to know about:*
>
> *(a) the purposes of the processing;*
>
> *(b) the categories of personal data concerned;*

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. (GDPR Art 15 (1a–h))

Negotiations about the range of personal data to be accessed

The GDPR states that, rather than refuse to provide all information concerning the data subject,

…Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates. (sic) See GDPR (63)

Redacting personal data from the data set

Practice Note

In the provision of counselling services, practitioners may possibly be able to negotiate with clients about the amount or range of material from the client's records to be disclosed to the client, for example if there are many records and the copying or electronic transmission of all the records would be onerous, or if there is information in the records for which disclosure would be detrimental to the client's health and wellbeing. However, it seems from the draft legislation that the support of a healthcare professional may be required to justify a refusal to disclose personal data to a client if the ground is that to do so would be detrimental to their health and welfare. See the ICO website www.ico.org.uk for further developments.

Back to contents

How and when a copy of data should be provided

There is now a responsibility to provide a copy of the personal data undergoing processing. It is possible for some of it to be redacted (for example, if it contains information about another individual who has not consented to the disclosure and it is not reasonable to comply with the subject access request without the individual's consent) or to limit the amount of information to be disclosed by negotiation with the data subject requesting access. The format of copies is not specified here.

> *3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.* (GDPR Art 15 (3))

There is an additional provision in (GDPR Art 15 (3)) that if the data are requested *electronically* (e.g. by email) then they can also be provided electronically.

The copy must be provided as quickly as possible and at the latest, within one month of receipt of the request.

Charging admin fees for copies of data

Practice Note

In most cases controllers will not be able to charge a fee to comply with a subject access request and copies shall be provided free of charge. If the request is manifestly unfounded or excessive, or if the individual requests further copies of their data, a 'reasonable fee' may be charged based on the admin costs. Please refer to the ICO website www.ico.org.uk for clarification of reasonable costs and fees.

Back to contents

7.3.2 Rectification of personal data

The GDPR Art 16 provides the data subject with a right to obtain the rectification of inaccurate personal data held about him or her, or to have incomplete data completed, including by means of a supplementary statement.

Practice Note

In the counselling professions, some clients report in the course of therapy that they feel that they have been hampered by the existence of perceived inaccuracies in their medical records, or they may feel that a record needs updating to reflect their current situation – for example, they may have had a psychiatric diagnosis and treatment for a mental illness some years back, but find that, even though they had made a full recovery, this may not have been reflected in their medical records. Under the GDPR provision, that client might be able to ask for corrections to any inaccuracies in their medical records, or to ask for the record to be updated by a supplementary statement.

There is also a duty on the controller to notify recipients of data about the rectification of data, see (GDPR Art 19)

7.3.3 Erasure of personal data

The GDPR Art 17 establishes a right to 'be forgotten' that is, erasure of the personal data from the records.

The data subject shall have the right to obtain erasure of personal data, without delay, if:

- *the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*
- *the data subject withdraws consent on which the processing is based... and where there is no other legal ground for the processing;*
- *the data subject objects to the processing ... and there are no overriding legitimate grounds for the processing (e.g. in the public interest or for safety or security etc.), or the data subject objects to the processing pursuant to direct marketing or profiling;*
- *the personal data have been unlawfully processed;*
- *the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;*
- *the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).* (GDPR Art 17)

Back to contents

See also:

> *A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.* (GDPR (65))

Article 8.1. refers to the consent of children. The right of erasure applies to children under the age of 16 who may have given consent for processing data when they did not fully understand the implications, and in situations where they now want the data erased, for example, from social media and the internet. For more on children and consent, please see Part 11.

There is also a duty on the controller to notify recipients of data about the erasure of data, see (GDPR Art 19).

7.3.4 Restriction of processing of personal data concerning the data subject

Article 18 of the GDPR provides the right to ask a controller for restriction of the processing of their personal data.

The controller must not process the restricted data (except to store them) unless the controller has the data subject's consent, it is for the establishment, exercise or defence of legal claims, it is for the protection of the rights of another person, or it is for reasons of important public interest of the European Union or a Member State. If the controller

wishes to lift a restriction, they must inform the data subject.

> *(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website.*
>
> *In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system. (GDPR (67))*

The grounds for requiring a restriction are:

> *(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;*
>
> *(b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;*
>
> *(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.* (GDPR Article 18)

There is also a duty on the controller to notify recipients of data about any restriction on processing of personal data, see GDPR Article 19.

7.3.5 Notification of rectification, erasure and restriction of processing personal data

> *The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Articles 16, 17(1) and 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.* (GDPR Article 19)

7.3.6 Data portability

Article 20.1 (b) of the GDPR provides that, if the data are processed by 'automated means' (e.g. electronically, or a video or other recording), and if the data subject has consented, or requires data portability under a contract, then the data subject should be able, without hindrance, to receive them in a 'structured, commonly used, machine-readable and interoperable format' and have the right to transmit them to another controller. (GDPR (68); Article 20 (1))

In addition, there is the right to ask one controller to transmit the personal data to another, where technically feasible. (GDPR (68); Article 20 (2))

Practice Note

As an example, this right might apply in situations where a practitioner has a criminal record check from the Disclosure and Barring Agency (DBS) and requires this to be transmitted to a new employer, organisation or agency. Note: Great care must be taken in dealing with DBS records as it is a criminal offence to make unauthorised disclosures.

7.3.7 Withdrawal of consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal and the right to object

Where personal data are being processed on the basis of consent, the data subject can withdraw their consent at any time. Controllers and processors must act on withdrawals of consent as soon as possible and must cease to process the personal data.

Where a person's data are processed under Article 6 (1e) (where processing is necessary to perform a task in the public interest or in the exercise of official authority) or Article 6 (1f) (where processing is necessary for a legitimate purpose of the controller or a third party), the GDPR provides the right under Article 21 for the data subject to object at any time to the processing of his or her personal data, including profiling.

If a data subject objects to their personal data being processed for direct marketing purposes (e.g. receiving marketing by post) the controller can no longer process the data (Article 21 (3)).

In all other situations, the controller must stop processing the personal data unless they can demonstrate that they have 'compelling legitimate grounds for processing the data which overrides the interests, rights and freedoms of the data subject', or that processing is for the 'establishment, exercise or defence of legal claims' (GDPR: Art 21 (1)).

Practice Note

These rights shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information. This is important for practitioners' therapy contracts.

7.3.8 Information about the existence of automated decision-making, including profiling, and the right not to be subject to a decision based solely on automated processing, including profiling

Article 22 (2) provides that, unless the processing is:

- subject to a contract between the data subject and the controller;
- is authorised by a law which also safeguards the data subject's rights and freedoms; or
- is subject to the data subject's explicit consent,

then

> *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.* (GDPR Article 22 (1))

7.3.9 To know how long the data will be stored, or the criteria for deciding this

Article 13 (2a) of the GDPR requires that the controller shall, at the time when personal data are obtained, inform the data subject of:

> *(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. (GDPR Article 13 (2a))*

Practice Note

This will be another essential ingredient of the contract between practitioner and client, or practitioner and research participant.

7.3.10 To be informed of the legitimate interests in the data pursued by the controller or by a third party (save where the data subject is entitled to protection of their personal data, e.g. for a child)

In order for a controller or processor to comply with the GDPR, it will be necessary for them to inform the data subject of any legitimate interests they are relying on to process the data subject's personal data. The data subject can then exercise their rights under the data protection legislation, for example, to object to the processing.

Note: There will be some situations and risk warnings where the data subject is a child or vulnerable adult, and so entitled to additional protection of their personal data, for more, please see Parts 10 (vulnerable adults) and 11 (children).

Back to contents

8. Consent in the context of data protection legislation

The Information Commissioner's Office (ICO) has published guidance to assist controllers and processors in demonstrating compliance with the requirements of the GDPR, see https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. In relation to compliance with the requirements for consent, see pages 59-64.

Consent in relation to adults is covered by GDPR (32–33) and Article 7.

For consent in relation to vulnerable adults, see Part 10 of this resource. For consent in relation to children and young people under the age of 18, see Part 11. There are special provisions for consent in the context of research, see Part 12.

Consent when discussed here assumes that the person concerned has the mental and legal capacity to give valid consent. For further discussion of capacity and consent see BACP's GPiA 029 Legal Resource: *Mental Health & Law within the Counselling Professions in England & Wales.*

The GDPR is very clearly worded on the issue of consent, and it might help here to break it down to its constituent elements (non-italics are used for emphasis):

> (32) *Consent should be given by a* clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement *to the processing of personal data relating to him or her, such as by* a written statement, including by electronic means, or an oral statement. (GDPR (32))

Elements of consent with examples relevant to the counselling professions

Consent needs to be:

- **a clear affirmative act** (i.e. a signature, a tick placed by the client in a box, a letter or email, or a clear statement of 'yes I agree' indicated clearly in a manner appropriate to the client) Note: Silence and pre-ticked boxes do not constitute consent.
- **unambiguous** (i.e. clearly applicable to the specific term agreed)
- **freely given** (i.e. not given under any form of pressure)
- **informed** (i.e. it will depend on the clarity and adequacy of the information given to the client)

Back to contents

- **specific** (i.e. a generalised consent is not adequate, consent needs to specifically name the things to which the data subject agrees)

- **given orally, or in writing, electronic or other form appropriate for the client** (i.e. use of sign language, or use of a pointing board, etc. may meet the client's needs).

Article 7 adds extra conditions in relation to consent:

- **the controller shall be able to demonstrate that the data subject has consented** (i.e. if consent is in writing, email or recorded, there is proof, but if consent is oral or in sign language, there should be a record of this in the file)

- **if the consent is given in a written declaration that concerns other matters, the request for consent must be clearly distinguishable from the other matters, in an intelligible and easily accessible form, using plain language** (i.e. a global consent to all the terms included in a therapy contract is not sufficient, unless it can be demonstrated that the client's consent to the data processing has been clearly and separately explained and agreed. Best practice, therefore, is to have a separate set of clauses in a therapy contract in compliance with the terms required by the GDPR and demonstrating the client's consent to data processing on those terms). (GDPR Art 7)

The GDPR goes on to explain how consent might be given, and this could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. *Silence, pre-ticked boxes or inactivity should not therefore constitute consent.* Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

For the full wording regarding consent, see (GDPR (32) and Arts 7- 8). There are special provisions for consent in the context of research, see Part 12.

Article 7 of the GDPR adds extra conditions for consent:

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

Back to contents

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. (GDPR Art 7)

9. Confidentiality in the context of data protection legislation

The whole of the data protection legislation is intended to protect the human rights and fundamental freedoms of the 'natural person' (see Glossary). At the same time, it seeks to make information flow efficiently and for lawful purposes, for example, health and social care, protection of the public by detecting and preventing crime, social, trade and business activities, etc.

Confidentiality, is part of the UK law, and also embodied in the human rights and freedoms in the European Convention on Human Rights https://www.echr.coe.int/Documents/Convention_ENG.pdf. For more information on confidentiality, see BACP's GPiA 014 Legal Resource: *Managing Confidentiality*. See also Bond and Mitchels (2014).

9.1 Anonymisation

Anonymisation is defined in the *Ethical Framework* as 'the removal of any information that would allow the person concerned to be identified or identifiable by any means from what is being communicated'.

Anonymised information ceases to be 'personal data' in the meaning of the GDPR, with all the associated legal requirements and protection when any means of identifying the person concerned has been genuinely and irreversibly removed. The GDPR is very clear:

> *The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person, or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This regulation does not therefore concern the processing of anonymous information, including for statistical or research purposes.* (GDPR (26))

See the *Ethical Framework* (BACP 2018) Good Practice, points 83-90 and Good Practice, points 55g, 78, 83a.

Back to contents

Practice Note

Failure to anonymise data adequately within the counselling professions can lead to a breach of trust with the person concerned and cause harm resulting in significant embarrassment, anxiety or distress. If there is any uncertainty about whether anonymisation will be sufficient to protect someone's identity, it is ethically and legally good practice to seek that person's explicit consent to use that information and for how that information will be used.

Anonymisation is different in meaning from 'pseudonymisation', a term used in current data protection regulations, see Part 9.2.

9.2 Pseudonymisation

'Pseudonymisation' is defined as:

> *the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (GDPR Article 4 (5)).*

Practice Note

An example of this would be where a client's contact details and the client's records are kept separately but linked with a reference number. Another possible example of pseudonymisation which probably frequently occurs in practice is where a supervisee discusses a client's case in supervision, and wishes not to identify the client, so refers to them only by their first name.

Pseudonymised information is regarded as personal data, and subject to the data protection law.

> *(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.* (GDPR (28))

Note: Anonymised data are not regarded by the GDPR as subject to the data protection law. However, pseudonymised data are 'personal information' and subject to the GDPR.

The GDPR goes on to consider the use and impact of 'identifiers' and what reasonable means are likely to be used to make a person 'identifiable', including the use of technology.

> *The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.* (GDPR (26))

10. Data protection legal provisions for vulnerable adults

Consent generally, and in relation to adults is covered by GDPR (32–33) and GDPR Article 7. See Part 8 for discussion of consent. There are no specific provisions in the GDPR for vulnerable adults, but reliance is placed on the protection of the GDPR in general, and on the internal law in the member countries relevant to capacity to consent and the protection of vulnerable adults.

In particular, attention should be given to clarity of communication and information giving, and in demonstrating explicit consent to data processing. Information should be given in simple, easily understandable language, and in a form appropriate to the adult concerned, which can include oral explanations and consent, provided that a clear record of the consent is retained. Where an adult lacks the mental capacity to consent to data processing, the relevant consent may be obtained from a person holding a Power of Attorney, or from the Court of Protection.

Back to contents

Vulnerability can arise in many ways, that is, from differences in ability, mental capacity and in the context of a person's life. See GPiA 030: *Safeguarding Vulnerable Adults within the Counselling Professions in England and Wales*. For mental capacity, see GPiA 029: *Mental Health and Law within the Counselling Professions in England and Wales*.

In England and Wales, mental health law and practice have been radically reformed – the Mental Health Act 1983 has been amended by the Mental Capacity Act 2005, the Mental Health Act 2007, and the impact of the United Nations Convention on the Rights of Persons with Disabilities, which came into effect in 2008, and pose far reaching challenges to our current mental health legislation. Once again, mental health law and practice are under critical review. In March 2015, the NHS set up the Mental Health Taskforce, chaired by Paul Farmer (Mind's chief executive) seeking the views of mental health service users, their families and professionals to develop a new five-year strategy for mental health, focusing on prevention, access, integration and attitudes.

The Department of Health also set up a consultation 'No voice unheard, no right ignored'. Following the Law Commission review of the Deprivation of Liberty Safeguards (DoLS), the Department of Health (DH) issued the new *Mental Health Act 1983 Code of Practice* (Department of Health 2015a) and there may be other revisions to follow which are relevant to the effective implementation of the Mental Capacity Act 2005. Currently the guidance is the *Mental Capacity Act 2005 Code of Practice* (MoJ 2007). There may be further reforms to the detention of people under S.s 135 and 136 of the Mental Health Act 1983. Watch out for possible further changes.

Vulnerability may arise as a result of a person's life experience, for example domestic violence, abuse, and other forms of suffering or intimidation. This is recognised in law in the context of protecting the victims of abuse and violence, and vulnerable witnesses in criminal trials, see GPiA 070: *Working with CPS Guidance on pre-trial therapy with adults*.

11. Data protection legal provisions for children

The law affecting the rights of children (defined as children and young persons under the age of 18) includes: the Children Act 1989 (1989); the UN Convention on the Rights of the Child (ratified by the UK in 1991); and the Human Rights Act 1998 (in force in the UK from 2 October 2000), which incorporates the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and its Protocols into UK law. Under s.7(1) of the Human Rights Act 1998, a person who claims that a public authority has acted in a way that contravenes the ECHR may bring proceedings against that authority.

In addition to law, there is a body of guidance, some of which is made under statutory powers and therefore carries a limited legal force. An example of this is *Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children* (DfE, 2018), is available at https://www.gov.uk/government/publications/working-together-to-safeguard-children--2 made under s.7 of the Local Authority Act 1970, and which should be followed by schools and local authorities in England and Wales (with sanctions for non-compliance) unless they can justify with good reason why they did not do so.

The law on children's capacity to make decisions, and other people making decisions for children, is vitally important for all practitioners who work with children and young people. Whether children can enter into a therapeutic contract will depend upon whether they have the legal capacity to make their own decisions. Consent generally, and in relation to adults is covered by GDPR (32–33) and Article 7. For consent in relation to vulnerable adults see Part 10. There are special provisions for consent in the context of research, see Part 12.

The provisions in relation to consent for the processing of personal data concerning children and young people under the age of 18 are governed by the GDPR (38). Article 8 GDPR and section 9 DPA also contain provisions relating to children's consent to the offer of 'information society services' (i.e. online services). See Part 11.2 for online services to children and Part 11.3 for direct services to children.

Although 'child' for all other purposes is not defined in the Glossary to the GDPR, the ICO adopts the same definition as section 105 of the Children Act 1989, and in European Convention on the Rights of the Child, i.e. a child or young person under the age of 18.

Back to contents

11.1 Law on children and consent in England Wales and Northern Ireland

Below is a very brief summary, for more detail see the BACP Legal Resource GPiA 031: *Safeguarding Children and Young People.*

Age 18 In the UK, Section 1 of the Family Law Reform Act 1969 lowered the former age of majority of 21 to the current age of 18. A minor (person under 18 years of age) may make a valid contract for 'necessary' goods and services, including counselling and medical services.

Age 16–18 Under s.8 of the Family Law Reform Act 1969, at the age of 16, a young person with mental capacity gains the right to give informed consent to medical or dental treatment, which includes psychological treatment and counselling. By implication, examinations or assessments are included in this. The consent of the young person is regarded as equally valid to that of an adult. However, in specific situations, the High Court has the power to overrule the decision of a young person if necessary for their welfare, for example, to save their life. A young person with mental illness, disability or psychiatric disturbance may also be subject to the Mental Health Act 1983.

Age under 16 A younger child may make their own decision, if they have the capacity to give or refuse informed consent under the common law set by the (then) House of Lords in the case of *Gillick v West Norfolk and Wisbech Area Health Authority and Another* [1986] 1 AC 112. For further details of the UK law regarding consent for children and young people, see Hershman and McFarlane's *Children Law and Practice Encyclopaedia ; and Working Together to Safeguard Children.* (DfE,2018)

The rationale of the Gillick case was that a child's ability to make an informed decision may be assessed according to a number of factors, including:

- the nature and seriousness of the decision to be made
- the child's age
- the child's maturity
- the child's understanding of the consequences of the decision, the circumstances and the context of the decision to be made
- the information given to the child to enable him or her to understand the potential benefits and risks of what is proposed and the consequences of consent or refusal.

Back to contents

It will be evident from the criteria above that the capacity of a child to make a decision is situation-specific and that, to have capacity, the child must have an informed understanding of the issues, including the risks and benefits involved and the consequences of refusal.

The ability to help a child make a decision will depend on the provision of age-appropriate information and explanations or answers to their questions. The more serious the decision, the greater the need for the child to possess sufficient maturity and understanding to evaluate his or her situation in its wider context. For this reason, the courts have steadfastly refused to set specific age limits to assess competence under the 'Gillick' guidelines.

Each case involving a child client must be decided on its own merits. If the child is under 16, it is the task of the practitioner, with other professional help if necessary, to talk through the situation with the child client. Together, they will need to explore and discuss the child's circumstances and the therapeutic or other options available, considering the possible outcome of each option open to the child, and then decide whether the child has the capacity to make the necessary decisions, including whether to enter into a therapeutic contract. The same process is necessary in the context of a therapeutic relationship when helping a child to assess whether they will require the practitioner to keep confidentiality or make a referral.

Consent for a therapeutic assessment or a therapeutic contract can be given for a young child under the age of 16 who is not 'Gillick competent' by:

- a person with parental responsibility for the child; or
- an order of the High Court, for example in its wardship jurisdiction pursuant to an order of a court at any tier in the Family Division, for example in the context of a care order, or a specific issue order.

If therapeutic treatment is considered necessary and the child or those with parental responsibility refuse, or if there is any issue about the competence of a child to make an informed decision, the matter can, if necessary, be referred for expert opinion and/or to the High Court. The High Court has the power to make an order in the best interests of the child and resolve disputes with a 'specific issue' order made under s.8 of the Children Act 1989.

Where a child is mentally ill or mentally disordered and unable to make a legally valid decision for himself or herself, the High Court (in its 'Wardship' jurisdiction) may provide consent on behalf of a person under 18.

Practice Note (and an important warning regarding approaching those with parental responsibility)

Please note that while it is good practice in most circumstances to obtain consent from all those who have parental responsibility for a child when this is required by law, there are some circumstances where it is not practicable or safe to do so. It may be impractical when the matter is urgent, and those with parental responsibility are living apart and one is not accessible. It may be unsafe where one or more person(s) with parental responsibility may pose a risk to the child or others if approached for consent. In these situations, where there may be a risk to the child or others, always seek appropriate legal or other expert advice before taking action.

11.2 GDPR law on children and consent to data processing for online services

Under the GDPR, there are specific provisions relating to children and consent for the processing of personal data concerning them.

See GDPR, Article 8, which relates to the offer of 'information society services' to a child. The term 'Information society services' broadly means 'online services' and is defined in the Regulation as:

> *any service normally provided for remuneration at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, at the individual request of a recipient of the service.* (Directive 98/48/EC amending Directive 98/34/EC)

> ***Article 8***

> ***Conditions applicable to child's consent in relation to information society services***

> *1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.*

> *Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. (Note: the provisions of the DPA as set out below).*

Back to contents

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child. (GDPR Art 8)

Practice Note

Note: Under section 9 of the DPA, the provisions regarding the age of consent set out in Article 8 of the GDPR to the provision of online services to children and young people is set at 13 in the UK. **Note: The provisions in Article 8 do not apply to preventive or counselling services, whether online or not, see Part 11.3 below.**

11.3 GDPR and children's consent to data processing for direct counselling or preventive services to children

Practice Note

Please refer to Part 11.1 for a brief discussion of the law in the England, Wales and Northern Ireland regarding consent for children. This law applies to the provision of counselling services, confidentiality and also (with the exception of online counselling services, see Part 11.2.1) it applies to consent for data processing. The GDPR makes a special provision for consent for processing data concerning children receiving 'preventive or counselling services offered directly to a child.'

*However, if a child is **not** competent within the Gillick guidelines to give his or her own consent, then it is submitted that the usual rules of obtaining lawful consent will apply.*

> *'Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.' (GDPR (38))*

This concept is reinforced by the ICO in its guidance on children, see: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf.

In therapy, we are not only contracting about data processing, we are also contracting for the provision of therapy with a child. For children who have the capacity to give consent, therefore, it is assumed that the Gillick criteria will apply and the consent of those with parental responsibility is not required (see Part 11.1), but for those children under the age of 16 who do not have the capacity to consent, the normal legal principles of consent for children will apply (see Part 11.1).

11.4 GDPR and children's right to require erasure of data, that is, 'to be forgotten'

The right to require erasure of data, that is, 'to be forgotten' applies to all data subjects, but in the case of children this right is specifically reinforced under the GDPR, to allow adults to require erasure of data in a number of circumstances, including when consent had been given when they were children, but that consent is now withdrawn. See Part 7.3.3 for discussion of the erasure of data generally.

> *A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of*

the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims. (GDPR (65))

11.5 Disclosure of data relating to children and safeguarding issues

Practice Note

Situations where client information may have special protection from disclosure, including response to requests from the data subject

Under Schedule 3 of the Data Protection Act 2018 there are listed exemptions to the general provisions of Article 15 of the GDPR regarding disclosures. Under these exemptions, data controllers may refuse disclosure of information about the data subject (e.g. including a disclosure to the data subject themselves, or to those with parental responsibility for a child who is a data subject), where the result of that disclosure could cause serious harm to the physical or mental health of the data subject or another individual (e.g. in child protection, medical, social work or educational situations). In this situation, it is best to seek appropriate legal advice and/or the assistance of a suitably qualified person. Part 5 of Schedule 3 of the Data Protection Act 2018 applies a separate additional exemption relating to maintaining the confidentiality of child abuse data.

Back to contents

Child's right to see their own records

Under data protection law, a child with capacity to make their own decisions has a right to see their own records.

If the child does not have the capacity to make his or her own decisions, then those with parental responsibility for the child will usually have the right to make decisions relevant to therapy, and under data protection law will also usually have the right to see the child's therapy records **BUT note that in this situation there are certain legal exceptions allowing the therapist and school to maintain secrecy, where this is necessary to safeguard the health or safety of the child or others, or to safeguard a police or other investigation in the context of child protection or crime. In these situations legal or other appropriate expert advice should be sought before data is disclosed to those with parental responsibility.**

Note that if a counselling record is regarded as part of the school record, then, under data protection legislation, those with parental responsibility may usually have a right of access to their child's records if the child is not competent to make his or her own decisions (in the context of the Gillick case), or if a competent child has not expressed his or her wish to have their confidentiality protected, **but the counsellor needs to be aware of the legal safeguards for information relating to child protection issues and other information that may, if disclosed, cause a risk to the child or others, or raise a police or safeguarding investigation. In these situations, legal or other appropriate expert advice should be sought.**

Back to contents

12. Data protection law in the context of research

The GDPR applies the same rules of fair and lawful data processing to research, as it does to other areas of data gathering and data processing. However, it does recognise that research is a process of continual development, and so it may be difficult, particularly in scientific research projects, to predict future purposes and outcomes. For this reason, consent to research, although it needs to be clear, unambiguous and explicit, may also need some degree of flexibility as a research project progresses. Regular review in co-operation with research participants may assist researchers to check the continuing validity and legality of participants' consent. The GDPR also envisages a limitation of the areas of research for which consent is given:

> *It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.* (GDPR (33))

For more detailed research guidance, see the BACP's *Ethical Guidelines for Research in the Counselling Professions* (BACP 2018).

Back to contents

13. Documenting and recording data protection compliance to meet legal requirements

Article 5(2) of the GDPR places heavy reliance on demonstrating compliance with the principles of the GDPR and makes it the responsibility of the controller and the processor to create a data processing system that leaves a clear trail of evidence to show compliance with the rules.

Controllers document all the applicable information under Article 30 (1) of the GDPR.

Processors document all the applicable information under Article 30 (2) of the GDPR.

The Information Commissioner's Office (ICO) has published guidance on documenting compliance with the GDPR, at https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (pages 168-173).

Records must be maintained on several things such as processing purposes, data sharing and retention, which may be required to be seen by the ICO on request.

Practice Note

Fortunately for most counsellors and psychotherapists, who will work in 'micro-organisations' in terms of the GDPR (see Part 14 for definitions and fees), documentation requirements will be limited to 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.

Back to contents

13.1 Best practice in documentation of processing activities – requirements

Practice Note

- Records must be kept in writing.
- Most organisations will benefit from maintaining their records electronically.
- Records must be kept up to date and reflect your current processing activities.
- The ICO has produced some basic templates to help to document processing activities.
- Those who need to record a client's criminal convictions and offence data have special requirements, see the ICO website at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance.

Preparation:

When preparing to document our processing activities we:

- do information audits to find out what personal data our organisation holds;
- distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and
- review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities we document, or link to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports; and
- records of personal data breaches.
- We document our processing activities in electronic form, so we can add, remove and amend easily. (ICO 2018) at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance.

Back to contents

The checklist below sets out the requirements for best practice in documenting compliance with the GDPR. For the relevant provisions in the GDPR, see (GDPR Art 28–36; and (81–83)).

Table 13A: Checklist: Compliance with the GDPR documentation process

- Written contracts between controllers and processors are required.
- These contracts must now include certain specific terms, as a minimum. The ICO is allowed under the GDPR to set standard contractual clauses, but none have been drafted so far.
- The GDPR allows the ICO to draft a Code of Conduct, or certification scheme for processors, to assist in contracting and compliance, but none have been drafted so far.
- A contract is needed whenever:
  - a controller uses a processor (a third party who processes personal data on behalf of the controller)
  - if a processor employs another processor it needs to have a written contract in place.
- Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

Contracts must require the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their obligations as a processor under (GDPR Art 28), and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.
- The consent of the data subjects should be documented clearly, see Part 8 for more on consent

Back to contents

14. Fees payable to the ICO

Fees are payable by 'controllers' to the ICO's office Data Protection (Charges and Information) Regulations 2018 in order to fund the administration of data protection:

> *Under the 2018 Regulations, organisations that determine the purpose for which personal data are processed (controllers) must pay the ICO a data protection fee unless they are exempt.* (ICO website at: https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf.

The fees will be calculated on the nature, activities and size of the business concerned. The lowest range of fees is currently set at £40 per annum (no VAT) and there is a discount of £5 for those who choose to pay by direct debit, but these fees may change, and watch the ICO website for any fee changes see www.ico.org.uk. For a list of exemptions, and for full information on the fee structure, see the guidance, which can be downloaded as a PDF and contains useful and clear information about the fees payable and answers frequently asked questions. The ICO guidance on fees and checklist are comprehensive and should be checked if any member is in doubt about what they should pay. There is also a helpdesk for small organisations, which can be accessed from the ICO website.

14.1 Fee structure summary

Below is information derived from the ICO guidance. For full details, please refer to the ICO document **Data Protection Fees for Controllers** at https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf.

> ***2. Overview of the 2018 Regulations***
>
> The new data protection fee replaces the requirement to 'notify' (or register), which is in the Data Protection Act 1998 (the 1998 Act). The ICO has the power to enforce the 2018 Regulations and to serve monetary penalties on those who refuse to pay their data protection fee.
>
> Although the 2018 Regulation came into effect on 25 May 2018, this doesn't mean everyone had to pay the new fee on that date. Controllers who have a current registration (or notification) under the 1998 Act do not have to pay the new fee until that registration has expired.
>
> Under the 2018 Regulations, controllers must pay the ICO a data protection fee unless an exemption applies – see 14.2.

Back to contents

3. How much is the data protection fee?

'There are three different tiers of fee and controllers are expected to pay between £40 and £2,900. The fees are set by Parliament to reflect what it believes is appropriate based on the risks posed by the processing of personal data by controllers. The tier you fall into depends on:

- *how many members of staff you have*
- *your annual turnover*
- *whether you are a public authority*
- *whether you are a charity*
- *whether you are a small occupational pension scheme.*

Not all controllers must pay a fee. Many can rely on an exemption.

***Tier 1 – micro organisations** You have a maximum turnover of £632,000 for your financial year or no more than 10 members of staff. The current fee for tier 1 is £40.*

***Tier 2 – small and medium organisations** You have a maximum turnover of £36 million for your financial year or no more than 250 members of staff. The current fee for tier 2 is £60.*

***Tier 3 – large organisations** If you do not meet the criteria for tier 1 or tier 2, you have to pay the current tier 3 fee of £2,900.*

We regard all controllers as eligible to pay a fee in tier 3 unless and until they tell us otherwise'.

(See ICO website at https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf.)

14.2 Exemptions

The 2018 Regulations make certain exceptions or fee reductions for some controllers. There are special rules for public authorities, charities and small occupational pension schemes.

Generally speaking, the fee must be paid if you are processing personal data as a controller. But there are some exemptions. You don't need to pay a fee if you are processing personal data only for one (or more) of the following purposes:

Back to contents

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Not-for-profit purposes
- Personal, family or household affairs
- Maintaining a public register
- Judicial functions
- Processing personal information ***without*** an automated system such as a computer.

The ICO then explains:

> *'If none of your processing is carried out on computer, a fee is not due. "Computer" includes any type of computer, for example cloud computing, desktop, laptop, tablet. It also includes other types of equipment which, although not normally described as computers, nevertheless have some ability to process automatically. Examples include automatic retrieval systems for audio and visual systems, electronic flexi-time systems, telephone logging equipment, CCTV systems and smartphones.'* (ICO website at https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf (accessed 2Jan 2019).

By working through the questions on the ICO website, you will be able to tell whether you need to pay the data protection fee.

Practice Note

BACP members should note two important things: maintaining records of our clients' contact details plus session records of our therapy work and supervision, i.e. processing personal data for the purpose of the provision of therapeutic services, is not likely to fall within the exemptions. The listed exemption for 'accounts and records' refers to records kept for purely accounting purposes, e.g. name, address and credit card details. Also, note that even if you process all data manually, and so are exempt from paying a fee, you still need to comply with your other data protection obligations.

For those in the counselling professions who are controllers, a fee will be payable, and exemptions are unlikely to apply.

Back to contents

15. Where to find ethical, professional or legal advice on data protection

Professional Ethics

In the counselling and psychotherapy professions, we may need advice or assistance on ethical or legal problems that arise in practice. If the problem is ethical, wherever possible and appropriate, consult your supervisor, and BACP has an Ethics Hub for members, which can be accessed by telephone or email – contact details are on BACP's website https://www.bacp.co.uk/about-us/contact-us/ethics-service.

Data Protection advice

If the problem is one of compliance with the GDPR, then the Information Commissioner provides access to advisers for personal help for small organisations, which can be accessed through the ICO website at https://ico.org.uk/global/contact-us where you can find a number of links: helpline, live chat, advice service for small organisations, and email.

For postal addresses, see the Head Office and Regional Office addresses below.

Head office

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.
Fax: 01625 524 510

ICO regional offices

Scotland

Information Commissioner's Office
45 Melville Street
Edinburgh
EH3 7HL

Tel: 0303 123 1115
Email: scotland@ico.org.uk

Back to contents

Wales

Information Commissioner's Office
2nd floor
Churchill House
Churchill way
Cardiff
CF10 2HH

Tel: 029 2067 8400
Fax: 0292 067 8399
Email: wales@ico.org.uk

Northern Ireland

Information Commissioner's Office
3rd Floor
14 Cromac Place
Belfast
BT7 2JB

Tel: 028 9027 8757 or 0303 123 1114
Email: ni@ico.org.uk

Legal advice

When seeking legal advice, search for a solicitor or lawyer who is suitably qualified and experienced in the topic on which the advice is needed. The professional legal websites usually list qualifications and experience, to assist choice. Legal advice can be expensive, and sometimes, for goodwill and public work, firms of lawyers will offer free (pro bono) advice sessions in their local Citizens Advice Bureau, local charity advice services and or at their offices. A list of these may be available through the Town Hall or local authority.

For legal advice from a solicitor in England and Wales, see the Law Society website, to find a solicitor at http://solicitors.lawsociety.org.uk

To find a solicitor in Scotland, see www.lawscot.org.uk/find-a-solicitor

To find a solicitor in Northern Ireland, see www.lawsoc-ni.org

Back to contents

Safeguarding children

If the advice required involves safeguarding issues concerning a child, the local authority legal service lawyers may be able to provide legal advice.

Government advice is available at www.gov.uk

Link not working

The NSPCC will provide advice and assistance, see www.nspcc.org.uk/prevent-abuse/safeguarding. And see https://www.nspcc.org.uk/what-you-can-do/get-advice-and-support (accessed 10 May 2018).

See also BACP Legal Resource sheets, GPiA 031 Legal Resource: *Safeguarding Children and Young People* and GPiA 029 Legal Resource: *Mental Health Law in England and Wales*.

Safeguarding adults

If the advice required involves safeguarding issues concerning a vulnerable adult, the local authority legal service lawyers may be able to provide legal advice.

For safeguarding vulnerable adults, see BACP's GPiA 030 Legal Resource: *Safeguarding Vulnerable Adults*.

For safeguarding adults in social care, see www.scie.org.uk/adults/safeguarding

Legislation referenced

Children Act 1989

Data Protection Act 1998 (repealed 25 May 2018)

Data Protection Act 2018

Data Protection (Charges and Information) Regulations 2018 (the 2018 Regulations)

General Data Protection Regulation PDF at http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

Data Protection (Subjects Access Modification) (Health) Order 2000 section 7, see https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request.

Freedom of Information Act 2000

Human Rights Act 1998

Back to contents

Mental Capacity Act 2005

Mental Health Act 1983

Mental Health Act 2007

Link not working

The key facts, articles and information about the implementation of the GDPR across Europe, are available at www.eugdpr.org/eugdpr.org.html.

About the author

The content author is Dr Barbara Mitchels, PhD, LL.B, BACP Registered (Snr Accred). She is a Fellow of BACP and the Director of Watershed Counselling Services in Devon. Barbara is also a retired solicitor, providing a consultancy service for therapists and CPD workshops around the UK.

Acknowledgements

The content author would like to thank David Membrey, MPhil, Dip Lib, DChA, a consultant with Adapta Consulting who has been supporting BACP through the process of GDPR compliance. I have enjoyed working with him in our co-authorship of articles on the GDPR for recent editions of BACP's Divisional Journals and appreciate his experience and advice in this field. Where relevant, some of our joint thinking on the potential implications of the GDPR in practice are reflected in this 2019 update.

In writing the original version, I also really appreciated the help and support of Tim Bond, and also Brethertons and Russell-Cooke solicitors, for their helpful comments on the original draft of this resource.

Back to contents

References

British Association for Counselling and Psychotherapy (BACP) (2018) *Ethical Framework for the Counselling Professions*. Lutterworth: BACP.

British Association for Counselling and Psychotherapy (BACP) GPiA 029 Legal Resource: *Mental Health & Law within the Counselling Professions in England & Wales*. Lutterworth: BACP.

British Association for Counselling and Psychotherapy (BACP) GPiA 014 Legal Resource: Managing Confidentiality. Lutterworth: BACP.

British Association for Counselling and Psychotherapy (BACP) GPiA 030 Legal Resource: *Safeguarding Vulnerable Adults within the Counselling Professions in England & Wales*. Lutterworth: BACP.

British Association for Counselling and Psychotherapy (BACP) GPiA 031 Legal Resource: *Safeguarding Children and Young People.* Lutterworth: BACP.

Bond, T. and Mitchels, B. (2014) *Confidentiality and Record Keeping in the Counselling Professions.* 2nd Edition. London: Sage.

European Parliament and the Council of the European Union The key facts, articles and information about the implementation of the GDPR across Europe, are available at https://europa.eu/european-union/about-eu/institutions-bodies/european-parliament_en. (accessed 19 February 2018)

DfE (2018) *Working together to safeguard children: a guide to inter-agency working to safeguard and promote the welfare of children.* Norwich: The Stationery Office. Available at: https://www.gov.uk/government/publications/working-together-to-safeguard-children--2 (accessed 02 Jan 2019)

Department of Health (2015a) *Mental Health Act 1983: Code of Practice* available at https://www.gov.uk/government/publications/code-of-practice-mental-health-act-1983. (accessed 14 October 2015)

Department of Health (2015b) *Code of Practice Mental Health Act 1983 Easy Read* available at https://www.gov.uk/government/publications/code-of-practice-mental-health-act-1983. (accessed 28 March 2018)

Department of Health (2013) *Caldicott Review: information governance in the health care system April 2013* https://www.gov.uk/government/publications/the-information-governance-review. (accessed 28 March18)

Back to contents

Hershman, D. and McFarlane, A. *Encyclopaedia of Children Law and Practice*. Loose Leaf. Bristol: Family Law.

Information Commissioner's Office (ICO) www.ico.org.uk.

ICO Data Sharing Code of Practice, see the ICO website at https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

ICO *Guide to the General Data Protection Regulation*. Available at: https://ico.org.uk/for-organisations/data-protection-reform. (accessed 19 February 2018)

ICO *On-line Self-Assessment tool*: (https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/ (accessed 02 March 2018)

ICO (2018a) *The Data Protection Fee. A Guide for Controllers*. Available at https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf) (accessed 02 March 2018)

Mitchels, B. (Ed) (2012) *Child Care and Protection: Law and practice*. 5th Edition. London: Wildy, Simmonds and Hill.

MoJ (2007) *Mental Capacity Act 2005 Code of Practice*.

Further reading and useful resources

Department of Health (2009) *Guide to Consent for Examination or Treatment*. London: Department of Health. Available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/138296/dh_103653__1_.pdf (accessed 19 October 2015).

Department of Health (2005) *Mental Capacity Act 2005: Deprivation of Liberty Safeguards – Code of Practice to supplement the main Mental Capacity Act 2005 Code of Practice*. 2008. Available at: https://www.gov.uk/government/publications/deprivation-of-liberty-safeguards-forms-and-guidance (accessed 10 May 2018).

The General Medical Council (GMC) provides ethical and legal guidance for doctors, including guidance on confidentiality and consent, see https://www.gmc-uk.org

Hale, B. (2010) *Mental Health Law*. 5th Edition. London: Sweet & Maxwell.

Back to contents

Jones, R. (2017) *Mental Capacity Act Manual*. 7th Edition. London: Sweet & Maxwell.

Long, M. (2014) *Child Care Law: A Summary of the Law in Northern Ireland.* London: BAAF.

Mason, J. and Laurie, G. (2006) *Law and Medical Ethics.* Oxford: Oxford University Press.

Mitchels, B., and Bond, T. (2008) *Essential Law for Counselling and Psychotherapists.* London. BACP and Sage.

Mitchels, B., and Bond, T. (2012) *Legal Issues Across Counselling and Psychotherapy Settings.* London. BACP and Sage.

Reeves, A. (2010) *Working with Suicidal Clients*. London: Sage.

Reeves, A. (2015). *Working with Risk in Counselling and Psychotherapy.* London: Sage.

Ruck Keene, A., Edwards, K. et al. (2014). *Court of Protection Handbook: A User's Guide*. London: Legal Action Group.

United Nations (2011) *United Nations Convention on the Rights of Persons with Disabilities 2011* (available at https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html) (accessed 13 May 2018)

United Nations *Convention on the Rights of the Child* (1989) (ratified by the UK in 1991) available at https://www.gov.uk/government/publications/united-nations-convention-on-the-rights-of-the-child-uncrc-how-legislation-underpins-implementation-in-england (accessed 13 May 2018)

Back to contents

Glossary

This resource refers to and is supportive of BACP's *Ethical Framework for the Counselling Professions* (BACP 2018) (the *Ethical Framework*). The Glossary as shown here includes definitions taken from the *Ethical Framework*, and *Ethical Framework Glossary* that are relevant to data protection. For other definitions relevant to the counselling professions, please see the *Ethical Framework Glossary* which can be downloaded from BACP at: https://www.bacp.co.uk/news/2018/16- april-2018-ethical-framework-review. Following each definition there is a link to the relevant section of the *Ethical Framework*.

link not working

C= Our commitment to clients.

E= Ethics.

GP= Good practice.

For example:

C2e can be found in the section *Our commitment to clients*, point 2, sub-point e.

The definitions given below explain the meaning of words used within this resource and in the *Ethical Framework*. Many of the words may be defined differently in other contexts. These definitions are provided as supplementary information and should be understood as non-binding good practice guidance, which do not override or weaken the commitments contained in the *Ethical Framework*. Definitions in this Glossary may be adapted or refined to suit particular services or settings, where any changes are consistent with the *Ethical Framework*.

A

Accurate
All due care has been taken about the truthfulness, completeness and exactness of what is being communicated (C2e, 5b, E12, GP15, 45, 71, 75). See also **Accurate records**

Accurate records
Records that are factually correct and complete and are careful to distinguish fact from opinion or interpretation (C2e, GP15, 71).

Back to contents

Anonymisation/Anonymised

Anonymised: The removal of any information that would allow the person concerned to be identified or identifiable by any means from what is being communicated. Failure to anonymise adequately within the counselling professions can lead to a breach of trust with the person concerned and cause harm resulting in significant embarrassment, anxiety or distress. Where there is any uncertainty about whether anonymisation will protect someone's identity, it is ethically and legally good practice to seek that person's explicit consent to use that information and for how that information will be used

Anonymisation is different in meaning from 'pseudonymisation', a term used in current data protection legislation. 'Pseudonymisation' is defined as:

> *the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person* (GDPR Article 4.5)

An example of this would be where a client's contact details and the client's records are kept separately but linked with a reference number. Pseudonymised information is regarded as personal data, and subject to the data protection law.

By contrast, anonymised information ceases to be 'personal data' with the associated legal requirements and protection when any means of identifying the person concerned has been genuinely and irreversibly removed. The GDPR is very clear:

> *The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person, or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This regulation does not therefore concern the processing of anonymous information, including for statistical or research purposes.* (GDPR (26)) *Ethical Framework* 2018 Good Practice 55g, 78, 83a.

Appropriate
Fitting and ethically right for its purpose. This term is widely used throughout the *Ethical Framework for the Counselling Professions*. See also **Appropriate records**

Back to contents

Appropriate records
Adequate, relevant and limited to what is necessary. The decision about what is appropriate will take into account the ethical and legal requirements for processing (includes making, keeping, using and sharing) records. See Information Commissioner's Office www.ico.org.uk for the latest information C2e

B

Breaching confidentiality
Disclosing something that has been communicated in confidence by mutual agreement or with the expectation that it will be kept secret. The expectation of secrecy may have been stated expressly or implied. Confidentiality is breached when any disclosure is made without the consent of the person concerned, legal authorisation or being legally defensible in the public interest. Breaches can occur accidentally or deliberately. In most circumstances, obtaining the consent of the person concerned provides an ethical way of avoiding a breach of confidentiality. Any disclosure of confidential information requires respecting the possible rights to confidentiality of any third person who is identifiable within the disclosure GP9

C

Children and young people
Anyone under the age of 18 years in the UK GP27a–d. See also **Safeguarding**

Circle of confidentiality
This circle represents the boundary between people who are included or excluded from the confidentiality agreement with the client. It encompasses all the people who have access to confidential information about clients as part of their usual work and are explicitly committed to treating that information as confidential, typically as a term of their employment. The people within the circle of confidentiality may be identified to clients by name or role, for example in contracting. The communication of confidential information beyond the circle of confidentiality will require client consent, being legally defensible in the public interest, or legal authorisation by court order or statute GP55b. See also **Confidentiality**

Computer
includes any type of computer, for example cloud computing, desktop, laptop, tablet. It also includes other types of equipment which, although not normally described as computers, nevertheless have some ability to process automatically. Examples include 'automatic retrieval systems for audio and visual systems, electronic flexi-time systems, telephone logging equipment, CCTV systems and smartphones.' (ICO: 2018) Available at: https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf (accessed 2 March 2018)

Back to contents

Client
A client is anyone in receipt of coaching, counselling, pastoral care, psychotherapy or counselling skills from a member or registrant of the British Association for Counselling and Psychotherapy. This includes being a supervisee or trainee. All clients are entitled to receive services that satisfy the commitments stated in this *Ethical Framework* in ways that are appropriate to the type of service being provided and its setting. Trainees, supervisees, and participants in research will receive the same applicable commitments and ethical standards as any client receiving services from a member of the counselling professions. This term is widely used throughout the *Ethical Framework for the Counselling Professions.*

Confidentiality
The protection of information that has been communicated in the expectation that it will be not be disclosed to others C3b, GP9, 10, 31c, 42, 44, 55a–g, 64. (See also Reasonably foreseeable limitations to confidentiality in the *Ethical Framework Glossary*).

Consent
An agreement to a course of action based on a shared understanding of what will be involved. In the General Data Protection Regulation 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement in the processing of personal data relating to him or her (GDPR (32); Article 4 (11); Article 7) GP16, 26, 27a, 28, 55f, 78, 83a, 88. See also **Informed consent**

Contract
Contract

An agreement, written or oral, between the people involved about the terms on which something (goods or services) will be provided. Any business and therapeutic terms and conditions that are agreed between counselling professionals and their clients will usually form part of the legal contract between them. Contracts may be useful in reinforcing and clarifying practitioners' ethical commitments to their clients and should generally be in writing, or in another form appropriate to the client's needs. It is good ethical practice to ensure that any contractual terms are clear and easily understandable and that the contract is readily available for the people concerned to check what has been agreed between them.

Back to contents

Controller
Defined in the GDPR Art 4 (7) as:

> *(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.* (GDPR Art 4 (7))

E

Explicit
Stated in words or clearly communicated by other methods, for example by sign language or images GP9, 88

I

Informed consent
Where the person giving consent is accurately informed about the reasonably foreseeable positive and negative implications in ways that that the person concerned can understand. In relation to processing personal information, data protection legislation sets a high standard for consent. See **Consent** GP26, 27a, 88 and also C6b, GP30, 49, 75

O

Online
Connected by computer or other digital technologies to communicate between people GP20

P

The data protection legislation applies to the processing of 'personal data'.

Personal Data: Defined in the GDPR Art 4 (1) as:

> *(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Back to contents

Processor

Defined in the GDPR Art 4 (8) as: '(8) "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'

Processing: Defined in the GDPR Art 4 (2) as:

> *(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

Pseudonymisation
'pseudonymisation' means the processing of personal data in such a manner additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person; (GDPR Art 4 (5))

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection

S

Safeguard(ing)
Protecting people's health, safety, wellbeing and human rights in order to enable them to live free from harm, abuse or neglect GP10, 55d

U

Unauthorised access or disclosure
This involves acting without legal authority or client consent to obtain or release confidential information in ways that are contrary to professional standards and ethics and violate the privacy of the people affected. Unauthorised disclosures may be deliberate or they may be accidental, for example by unintentionally leaving notes or a file in a public place. GP55a

Back to contents

V

Vulnerable adult
The meaning of 'vulnerable adult' varies across different contexts but is widely used to refer to people over 18 years old who are regarded as vulnerable because they are unable to adequately protect themselves against significant harm and exploitation or unable to take care of themselves without assistance.

In social policy, a vulnerable adult is typically someone aged 18 years or older, who is receiving or may need community care services due to mental or other disability, age or illness and who is or may be unable to take care of him or herself without assistance, or unable to protect him or herself against significant harm or exploitation.

The legal definition of a vulnerable adult in England and Wales is anyone to whom health and social care is being provided as set out in the Safeguarding Vulnerable Groups Act 2006 (as amended by the Protection of Freedoms Act 2012) GP28.

Back to contents