BRITISH/
PSYCHOANALYTIC
/COUNCIL

General Data Protection Regulation

Frequently Asked Questions

March 2024

What is the General Data Protection Regulation?

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR), and controls how personal information is used by organisations, businesses or the government.

Everyone responsible for using personal data has to follow a set of '**data protection principles'** which ensure that personal data is processed lawfully.

Those who hold personal data must make sure that the information is:

- used fairly, lawfully and transparently.
- used for specified, explicit purposes.
- used in a way that is adequate, relevant and limited to only what is necessary.
- accurate and, where necessary, kept up to date.
- kept for no longer than is necessary,
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

When did GDPR come into force?

The new regulations came into force on 25 May 2018. UK GDPR remains in force despite "Brexit" and the UK leaving the European Union.

Who will enforce the regulations?

The Information Commissioner's Office (ICO) is the regulator responsible for overseeing and enforcing the regulations. Individual data subjects (i.e. the people whose personal data is held and used by others) may also bring claims against the parties that hold and process their personal data for breach of their GDPR rights.

Does GDPR apply to me in private practice?

The new regulations apply to anyone who processes personal data about a UK citizen and to any data processing undertaken by organisations that are established within the UK, even if the data subjects themselves are outside the UK. It will apply to the personal data that you hold about your clients[1], and personal data in relation to employees and suppliers.

What is personal data?

> The ICO's website provides this following definition for personal data:
>
> The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both personal data in electronic form (including where such personal data is processed by automated means) and to manual filing systems where personal data are stored and retrieved for use. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on whether the party holding it has access to the key or how difficult it is to attribute the pseudonym to a particular individual.

Personal data may come from emails, social media interactions, recorded phone messages, as well as being held in formal records such as client's clinical records.

What is special category personal data?

Special Category Personal Data – This is a new definition that extends the concept of "sensitive personal data" to data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation. Owing to its sensitive nature, this data must be subject to more stringent controls and protected with a higher level of security. Personal medical information is special category data, hence these extra obligations apply generally in healthcare.

[1] The term "client" refers to both client and patient in this document.

I'm concerned about my lack of understanding of the new legislation. What should I do first?

In order for you to comply with the new regulations you need to understand what personal data you hold/handle. Carry out an information audit, this is merely noting and recording the nature, origin and destination of any personal data that you hold or share. You could think of the following questions whilst carrying out your audit.

1. Why am I holding this type of personal data and do I need to keep collecting such data in the future?
2. How long should I hold this personal data, and should I have already disposed of it?
3. How do I justify holding such personal data?
4. Are the third parties, that I share personal data with GDPR compliant? (Third parties may be people such as your accountants or IT support etc.)

Carrying out such an information audit, shows that you have carried out a risk assessment of the personal data (including special category data) that you hold.

The next step is to understand some of the GDPR language

The **Data Controller** determines the purposes and means of processing personal data. For the purposes of the GDPR, if you are working independently in private practice, it could be reasonable to assume that you would be the data controller when handling personal data about your clients and staff and determining what to do with it. If you are working in a clinic or a group practice it may be that the clinic will be the data controller. Organisations may have data processors to assist in processing the data on their behalf.

A **Data Processor** is any person who processes personal data on behalf of the data controller and on their instructions but does not decide the purposes and means of processing.

What is data processing?

Processing includes the 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 or personal data. If you undertake any of these activities on personal data, then that data processing must be undertaken in compliance with the GDPR.

Lawful basis for data processing

Under the GDPR, you must have a **valid lawful basis** in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others. Most lawful bases require that the processing is 'necessary'. If you can reasonably achieve the same purpose without processing personal data, you won't have a lawful basis. And to comply with the accountability principle under the GDPR you must be able to demonstrate that a lawful basis applies. You must also determine your lawful basis before starting to process personal data. It's important to get this right first time.

The ICO website states the following:

> The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:
>
> a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
> b) **Contract:** the processing is necessary for the performance of a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
> c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
> d) **Vital interests:** the processing is necessary to protect someone's life.
> e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
> f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

If you need further information in relation to these definitions or terminology, please see the BPC's earlier briefing or visit the ICO website.

Which lawful basis should I choose?

The BPC are unable to advise you on what lawful basis you should choose in relation to individual circumstances. However, where there is no contract in place you may be limited to the lawful basis of either consent or legitimate interest. It is important to note the following guidance given by the ICO which is helpful in relation to choosing between the two. Please note it will be your responsibility to ensure you have chosen the correct lawful basis.

> If you are processing for purposes other than legal obligation, contract, vital interests or public task, then the appropriate lawful basis may not be so clear cut. In many cases you are likely to have a choice between using legitimate interests or consent. You need to give some thought to the wider context,
> including:
>
> - Who does the processing benefit?
> - Would individuals expect this processing to take place?
> - What is your relationship with the individual?
> - Are you in a position of power over them?
> - What is the impact of the processing on the individual?
> - Are they vulnerable?
> - Are some of the individuals concerned likely to object?
> - Are you able to stop the processing at any time on request?
>
> You may prefer to consider legitimate interests as your lawful basis if you wish to keep control over the processing and take responsibility for demonstrating that it is in line with people's reasonable expectations and wouldn't have an unwarranted impact on them. On the other hand, if you prefer to give individuals full control over and responsibility for their data (including the ability to change their mind as to whether it can continue to be processed), you may want to consider relying on individuals' consent.
>
> https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis- for-processing/

Are there different rules to processing special category personal data?

It is important to note when processing special category personal data there are further requirements. This is due to the fact that the sensitive nature of the data requires more protection. In order to lawfully process special category personal data, you must identify both a lawful basis under Article 6 as stated above and a separate condition for processing special category data under Article 9. These do not have to be linked.

There are ten conditions for processing special category data in the GDPR itself, but be aware the Data Protection Bill will introduce additional conditions and safeguards.

The additional conditions can be found here: Special category data | ICO

If I am relying on consent as my lawful basis, what do I need to be aware of?

Consent means offering individuals **real choice** and **control**. Genuine consent should put individuals **in charge**, build trust and engagement, and enhance your reputation.

- Check your consent practices and your existing consents. Refresh your consents if they don't meet the GDPR standard.
- Consent requires a **positive opt-in**. Don't use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and **specific statement of consent**.
- Keep your consent requests separate from other terms and conditions.
- Be **specific** and **'granular'** so that you get separate consent for separate things. Vague or blanket consent is not enough.
- Be **clear and concise**.
- Name any third-party controllers who will rely on the consent.
- Make it easy for people to **withdraw consent** and tell them how.
- Keep **evidence** of consent – who, when, how, and what you told people.
- Keep consent under **review** and refresh it if anything changes.
- Avoid making consent to processing a **precondition** of a service.

What should I do once I have established my lawful basis for processing data?

Once you have established what personal data you hold and whether you have a lawful basis for processing that personal data, you will need to think about registering with the Information Commissioner's Office (ICO).

Do I need to register with the ICO?

With limited exceptions, most individuals that process personal data are obliged to register as a data controller with the ICO and will need to pay the ICO a fee (unless exempt).

The ICO breaks the fee categories down in 3 Tiers:

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 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 fee for tier 2 is £60.

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

ICO guidance states that if none of your processing is carried out on a computer, a fee is not due. Please find further details here.

What else do I need to be aware of?

The GDPR brings in enhanced data subject rights and greater accountability for data controllers and processors. Transparency is key!

The GDPR provides the following rights for individuals:

The right to be informed

- You must provide privacy information to individuals at the time you collect their personal data from them. You may address this by providing a privacy notice. (You can find the ICO's privacy notice here).
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
- There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and in plain language.

The right to access

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access requests. (You should have a system or process in place to deal with such requests.)
- Individuals can make a subject access request verbally or in writing.
- You have one month to respond to a request.
- You cannot charge a fee to deal with a request in most circumstances.

The right to rectification

- The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- You have one calendar month to respond to a request

The right to erasure

- The GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- Individuals can make a request for erasure verbally or in writing.
- You have one month to respond to a request.
- The right to erasure is not absolute and only applies in certain circumstances. See how it applies here Right to erasure | ICO
- This right is not the only way in which the GDPR places an obligation on you to consider whether to delete personal data.

The right to restrict processing

- Individuals have the right to request the restriction of processing or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances. See how it applies here.
- When processing is restricted, you are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- You have one calendar month to respond to a request.

The right to object

- The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.

- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies, you may be able to continue processing if you can show that you have a compelling reason for doing so.
- You must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.
- You have one calendar month to respond to an objection.

There are further rights which could be relevant that you can find on the ICO website.

Remember some of the rights stated above will not be absolute and will have exceptions, always check the ICO website on the circumstances where you may not have to comply with the above rights. If a data subject is unhappy with your processing of their personal data or your response to a request to exercise their rights, or to a complaint then they may complain to the ICO.

Sharing personal data

You will often need to send the personal data that you hold to other parties. This might involve sending payroll details to a payroll services provider, discussing the cases of minors with their parents, sharing information with others who also provide care to your clients.

The formalities associated with such data sharing will depend upon a number of factors, including whether the third party is your data processor or a data controller in their own right.

The personal data of a child belongs to that child and, if the child has capacity to consent or otherwise to the processing of their personal data then the wishes of the child may override any authority given by the parent or legal guardian. [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/]

In some instances, particularly in matters where an individual's vital interests are at risk, the processing is necessary and consent cannot be obtained, it is lawful to share personal data (including special category data) without consent. In other circumstances, you must be certain that personal data can be shared lawfully before proceeding without consent.

Before sharing data, you must be confident that the recipient will comply with their GDPR obligations and the terms of your contract with them (the GDPR requires that controller-to- processor arrangements are subject to a written contract that includes certain terms) and also that the data will be transferred and held securely.

How long should I keep records for?

The BPC are unable to provide advice in relation to how long clinicians should retain client notes as we understand that every clinician has different work practices. However, the general rule under the GDPR is that personal data should not be retained for longer than is necessary for the purpose for which it is collected.

You may be obliged to keep certain records for legal or regulatory compliance. These include records relating to the deduction/payment of taxes, pensions, corporate documents, right to work checks, etc. You may also need to retain certain information in connection with your insurance and you may want to retain personal data in connection with possible future court proceedings. For example, documents associated with a contractual relationship may be relevant until the end of the period during which a legal claim may be made in relation to the contract (this is often 6 years from the end of the contract, but can be longer). If retaining records for these reasons, it is necessary to check whether personal data must necessarily be held, or whether an anonymised/redacted document will suffice.

You may want to keep in mind the period in which the BPC can receive a complaint in relation to your conduct. The BPC's fitness to practice procedure states the following; *" The BPC will not consider complaints where the alleged conduct took place more than five years ago unless it is in the public interest to investigate the allegation"* [2]

NHS records have specified periods of retention, with client records there is no set time limit to keep records or for destroying them. It is important for you to decide on appropriate time limits for holding personal data, this could be different for each client and bearing in mind different circumstances.

The GDPR also requires data controllers to maintain records of their processing activities, so that you can show compliance. It can be a good idea to review all the personal data that you hold and dispose of anything that you shouldn't be holding. Carry out an assessment of what personal data you have and why and record this to show compliance. Ensure that client records are sufficiently protected and stored in a secure place to avoid data breaches.

Remember to state clearly from the outset to the individual whose personal data you hold, what your retention policy is, what you are keeping, why and the length of time you will be keeping it. If for any reason you are unable comply with the disposal of the notes, record this for your own recollection.

Requests for clinical records

[2] Appendix-1-Acceptance-Criteria-updated.pdf (bpc.org.uk) Paragraph 19B

You will occasionally be asked to provide your notes to the police or solicitors and this can lead to stress and anxiety. The BPC recommends that you speak to your insurers and obtain legal advice from their legal team. It is always advisable where consent is obtainable to try and get this from the individual before sharing the information. Remember to remove any information in relation to third parties. Unless the requesting party has a basis in law for demanding disclosure, your duty of confidentiality and the rights of the data subject may outweigh the reason behind the disclosure request. See further FAQ guidance on this topic from the BPC.

What if a client requests their notes?

A client has the right to request access to the personal data that you are holding about them. This is referred to as a subject access request. Ensure that you have procedures in place to deal with such requests within one month of receipt. You will not be able to charge for supplying this information. If you have any doubt as to the requesters identify or right to receive the data, then you may make reasonable further enquiries. In complying with a subject access request, it is important not to disclose the personal data of another person without that other person's consent.

> https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation- gdpr/individual-rights/right-of-access/

What if there is a breach of personal data?

The ICO defines a personal data breach as the following, "A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data." If a personal data breach occurs and there is a risk to the rights and freedoms of individuals, then you must notify the ICO within 72 hours of becoming aware of the breach. You may also need to notify the individual concerned in relation to the data breach. It is recommended that sensitive records (including special category personal data) are kept separately in a locked drawer or filing cabinet if in hardcopy and on encrypted, password-protected systems if held electronically. Special category personal data must never be kept on laptops, or portable storage (such as USB drives) unless the device or the file has been encrypted or password protected.

Summary

a) Carry out an information audit and dispose of any data not required. (Ask yourself the reasons to why you are holding the data and your lawful basis.)
b) Record your lawful basis for processing. (Don't forget special category personal data has further conditions.)
c) Prepare your privacy notice and ensure that it provides the right information. (Further guidance on drafting your privacy notice can be found here: How should you write a privacy notice? | ICO
d) If you are relying on consent, then ensure that you are fully compliant with how the consent should be documented and obtained.
e) Make sure you have policies and procedures in place for dealing with data access requests, data breaches and your obligations under the GDPR.

Important Note

The BPC are unable to provide clinicians with direct legal advice in relation GDPR compliance, the regulations do not provide definitive guidelines and the ICO are still providing guidance. Under the GDPR everyone is accountable for the data that they hold so it is important that you make your own assessment. The BPC is not responsible for the personal data that you hold. The information contained in this document is for general guidance only and cannot be relied upon as legal advice. The BPC accepts no liability for the accuracy of the information contained herein and you should always obtain specific legal advice separately before taking any action based on the information provided herein or if you are unsure as to how to act in any situation.

For further guidance please visit the ICO website Guide to the General Data Protection Regulation (GDPR)