# Why the GDPR?

This document is designed for those solopreneurs and sole traders who want to feel that GDPR compliance should have more steps to it and feel more serious. Enjoy.

At the heart of GDPR is protection of the individual.

This means protection for ordinary people against organisations collecting:

- All sorts of weird data (that they don't actually need)
- From all sorts of unknown places
- Using an algorithm to profile individuals and treat them differently
- … and ruining your life:
    - Acting on false data as fact
    - Spreading false or embarrassing data (by accident or deliberately)
    - Blocking you from access to credit rating, products, services, respect

So that *you* can't accidentally do those nasty things in the normal course of your work, and so that you can't get falsely accused of it either you need to make sure that:

- you don't trick people into consenting to stuff
- you know what you're doing and explain it clearly
- you give clear ways for people to access their rights
- you only deal with services that are playing by the same rules

<u>This is how to control what you do with people's data.</u>

In a big organisation, one person would decide the methods (be Data Controller) and the rest would be data processors.

Here are the steps that must be taken by Data Controllers. You can also follow these on the ICO website:

1. Be lawful fair and transparent

   *Don't just do it right, put it in print so people can see you do it right*

2. Look after the rights of the individual

   *Give clear and simple ways to contact you, have a real choice, object, change details etc*

3. Be accountable and responsible

   *Have a data protection policy – a list of how you keep people's data safe*

4. Keep things secure

   *Have a plan B – know what your weak points are and what to do if there is a problem*

In this document these four simple elements are colour coded for fast scrolling. The following overviews of each element are followed by more in-depth explanations of how to achieve the goals they contain.

For more detail or specific questions, please join us in our closed **Facebook Group**

**To be lawful fair and transparent :**

1. Know what personal data flows through your business, and how
2. Know your legal reasons/rights for each type of data
3. Register with ICO

Points 1 and 2 will both end up as part of your **privacy policy** which must be on your website and on any formal documents you send to clients.

Really you should have a privacy policy already. GDPR just adds bits to it. We will give you a fill-in-the-blanks practitioner privacy policy to edit, but first there is some information you need to get in one place.

**To look after the rights of the individual:**

It depends on your legal reasons whether these all always count:

- Right to know what data you collect, why and where it goes
- Right to understand – e.g. explain to children in their terms
- Right to access what you hold on them
- Right to make corrections & completions

- Right to be forgotten / erased from file
- Right to restrict processing ('keep it but don't use it')
- Right to data portability (e.g. taking their case notes to a new therapist)
- Right to object – especially to being on a mailing/marketing list
- Right to speak to a human being (and not be profiled by a robot)

**To be accountable and responsible:**

- Accountability – for yourself / your staff – have a data protection policy
- Contracts – with any processors (other people or businesses) so that they are legally responsible
- Watch out for information risks – keep a log, take counter steps
- List how you protect data – e.g. virus checker, locked cabinet
- Protection – assess the impact before using any new system or software

**Keep things secure:**

- Security – for yourself / your staff – have an information security policy – what you store where, why, and what to do if it goes wrong
- Damage limitation – know whether, when and why to report a data breach or loss of data
- International safety – make sure your US / non-EU processors comply with the law

# Lawful, Fair and Transparent

Knowing what personal data flows through your business:

A way to know what information flows through is to do an information audit

You can do this like a list or a graphic or a mindmap. It might help to think of it as getting clear on all the client funnels you have.

The very first time you get someone's name and email, or name and expression of interest, where does that come from? By phone? By email? Through a sign-up button? It could be many ways. Where do you store it?

How do you fill and keep your intake form? Your case notes?

Legal reasons:

- Consent: the client said yes.
- Contract: working together or providing/receiving a service
- Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests: to protect someone's life.
- Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, with a clear basis in law.
- Legitimate interests: yours or those of a third party e.g. making sure you get paid, seeing what marketing works best (unless the client's legitimate interests are bigger)

Consent for adults:

- Keep your consent requests prominent – not on the terms and conditions.
- Use positive opt-in such as unticked opt-in boxes – no joining by accident.
- Avoid making consent a precondition of service. No more "purchasing our service means you agree to receive our newsletter too"
- Allow clients to consent separately to different purposes and types of processing wherever appropriate.
- Name your business and any specific third parties who will rely on this consent so they know what they are signing up for.

- Keep records of what an individual has consented to, including what you told them, and when and how they consented.
- Tell individuals they can withdraw consent at any time and how to do this.
- Have systems to record and manage ongoing consent

Consent for kids:

Offering online services directly to children:

- Only kids over 13 can give their own consent
- Make sure everyone trying to give consent is really over 13

- For children under 13 you need to get consent from whoever holds parental responsibility for the child - unless the online services you offer are for preventive or counselling purposes.
- Make sure the person giving consent does have parental responsibility

Legitimate interests:

- E.g. marketing, increasing sales, improving systems and services.
- Needs a three part test:
    - **Purpose test** – is there a legitimate interest behind the processing?
    - **Necessity test** – is the processing necessary for that purpose?
    - **Balancing test** – is the legitimate interest overridden by the individual's interests, rights or freedoms?
- Balance – the individual's rights or freedoms – e.g. children's rights – make sure you are not treading on these
- Example of overstepping the mark: Target marketing personal problems on social media and 'outing' sufferers.

# Rights of the individual:

Recap: It depends on your legal reasons whether these all always count:

- Right to know what data you collect, why and where it goes
- Right to understand – e.g. explain to children in their terms
- Right to access what you hold on them
- Right to make corrections & completions
- Right to be forgotten / erased from file
- Right to restrict processing ('keep it but don't use it')
- Right to data portability (e.g. taking their case notes to a new therapist)
- Right to object – especially to being on a mailing/marketing list
- Right to speak to a human being (and not be profiled by a robot)

Right to know what data you collect:

You should publish this privacy information on your website and within any forms or letters you send to individuals:

- The name and contact details of your organization, & your representative (if applicable). Contact details of your data protection officer (if applicable).
- The purposes of the processing and the lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data. including details of transfers of the personal data to any third countries or international organisations.
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing including the right to withdraw consent (if applicable) and the right to lodge a complaint with a supervisory authority, e.g. your association or insurers.
- The source of any personal data not obtained from the individual it relates to.

- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

When to give this info:

Provide individuals with privacy information **at the time** you collect their personal data from them.

If you obtain personal data from a source other than the individual, provide them with privacy information:

- within a reasonable of period of obtaining the personal data and no later than one month;
- If you plan to communicate with the individual, then at the latest, when the first communication takes place; or
- If you plan to disclose the data to someone else, at the latest, when the data is disclosed.

Right to understand:

Avoid legalese when dealing with children. They have a right to understand the privacy information, age restrictions etc, even if they are getting permission from their parents.

Keep it simple, clear and plain English but explain everything as you would for an adult privacy policy.

Right to access:

Individuals have the right to obtain:

- confirmation that you are processing their data;
- access to their personal data; and
- other supplementary information

This largely corresponds to the information that you should provide in a privacy notice.

There are rules that apply to how fast you answer, how you answer and whether you charge a fee and these are covered in the template privacy policy which I have created for you.

Rights to make corrections:

- You must think of, and preferably write out, the methods you will use to make sure the info you hold on your clients remains up to date. We all forget which way we said we'd do something and its useful both as a memo and to prove you are on the ball if there is ever a complaint.
- Clients have the right to insist on updates, completions and corrections.
- The same rules about speed etc apply as before

Right to be forgotten:

- Make sure you have a set process for deleting client info when it is no longer required or when consent is withdrawn or the individual has asked you to erase it.
    - Examples – invoice and payment details after the six years for accounting purposes, personal details after the six years for case notes, name and email immediately from any marketing email list.
    - If you retain someone's contact and purchase details as a bad debtor, in order to keep a list of clients that you would not re-engage and for no other purpose, this would be a legitimate interest where the client may have no right to be forgotten. If you are sharing that negative information with other business, then the client would have a case.

Individuals have the right to be forgotten and can request the erasure of personal data when:

- no longer necessary for the original purpose you collected/ processed it for
- they withdraw consent;
- you rely on legitimate interests as a reason, they object and you have no overriding legitimate interest to continue
- you are using the data for direct marketing and the individual objects
- it was unlawfully processed (ie otherwise in breach of the GDPR)
- it has to be erased in order to comply with a legal obligation; or
- it is processed for information society services to a child.

(Rules apply as before)

Right to restrict processing:

When processing is restricted, you can store the personal data, just not process it. You can keep just enough information to make sure the restriction is respected in the future.

As a matter of good practice, you should consider restricting (pausing) the processing of personal data anyway, if:

- Someone contests the accuracy of their data, until you have checked its right.
- Someone has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your legitimate grounds override theirs.
- Processing is unlawful and the individual opposes erasure and requests restriction instead, so that you have a note on file to never do it again.
- You no longer need the personal data but the individual requires the data to be retained to allow them to establish, exercise or defend a legal claim.

Right to data portability:

This doesn't really apply to us as 1:1 therapists because that part of our business is not automated.

If you are a phone company and someone wants to switch providers and take their account history and call history with them, you have to have a way to send the lot over safely as an encrypted csv file or similar, so it goes straight from computer to computer.

- The right to data portability only applies to:
    - personal data the individual gave you themselves
    - and that is based on their consent or for the performance of a contract
    - and the processing is carried out by automated means.

Usual rules apply

Right to object:

Sometimes people have a right to object depending on your purposes and lawful basis for using their data.

- People have an absolute right to object to processing (including profiling) for direct marketing and you must stop as soon as you receive the objection. There are no grounds to refuse.
- A person can object, based on their particular situation, to processing (including profiling) for:
    - your legitimate interests;
    - the performance of a task in the public interest; or

    - exercise of official authority.

- Then you must stop processing the personal data unless:
    - you have strong legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
    - It is information you need to take to court as part of a legal wrangle.

The right to object is more restricted re: personal data used for scientific/historical research or statistics. If processing is necessary to perform a task in the public interest then there can be no objection.

Right to speak to a human being:

- It is not okay to decide who someone is based on their online data. The only time you can 'profile' someone like this purely online without speaking to them is when:
    - It is for entering into or performance of a contract between you and the individual;
    - It is authorised by law (e.g. for preventing fraud or tax evasion); or
    - It is based on the person's explicit consent.
- Even then, you must give the person clear ways to:
    - Get human intervention
    - Express their point of view
    - Obtain an explanation of the decision and challenge it

# Accountable and responsible

Data Protection Policy

The GDPR requires you to show how you comply with the principles of the new law.

Creating a policy will help you address data protection in a consistent manner and demonstrate accountability under the GDPR. This can be a standalone policy statement, a one page reminder sheet addressed to yourself.

If you have staff you also need a way to check that the systems are working and the policy is being kept

Contracts with processors (other people or businesses)

Whenever you use a processor (hire someone who is not staff to do the number crunching or to contact people on your behalf or to store the data or use it for profiling) unless there is a special legal act that applies, you need to have a written contract.

The contract is important so that both parties understand their responsibilities and liabilities.

The GDPR sets out what you need to be include in the contract.

You are directly liable for their compliance with the GDPR with respect to the client data that you have collected. You also need to be able to demonstrate that compliance for yourself and for your processors.

Failure may mean fines, penalties or legal proceedings.

You must only appoint processors who give 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

Processors must only act on your documented instructions but they do have some direct responsibilities under the GDPR and they too can be liable to pay damages in legal proceedings, or be subject to fines or other penalties or 'corrective measures'.

Handling other information risks:

Watch out for information risks – keep a log, take counter steps

List how you protect data – e.g. virus checker, locked cabinet

Assess the impact on safety before using any new system or software.

# Being Secure

The great thing about GDPR is that is accepts that even the best systems are rarely watertight. For that reason it asks you to have steps in place against a time that something goes wrong.

## Information Security Policy

It is sensible to have an information security policy that includes things like keeping your computer's anti-virus and anti-malware software up to date – including when they run out and what they cost. These are legitimate business expenses.

Again this only has to be a one page document written for your own peace of mind and kept up to date.

## When to report

If you hold someone else's personal data and somehow you destroy it, lose it, change it or share it, that is a breach.

You must keep records of when these accidents happen, this is also useful as proof that you are tightening up your systems. However you ***only have to tell the ICO*** if it is going to result in a risk to the rights and freedoms of the individual or individuals concerned.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must also notify those concerned directly and without undue delay.

## International Processors

When you contract to use processors within the EU, as covered under 'Safe and secure', you have to have a contract with them and you have to stand as legally responsible and liable for what they do with your clients data.

You may only transfer personal data outside of the EU if you comply with the conditions for transfer set out in Chapter V of the GDPR.

This is where it finally gets really heavy. As micro businesses and responsible practitioners we are not going to be sharing any sensitive data – at most names and emails to an autoresponder such as Mailchimp or Aweber.

The most likely reason for being able to use non EU services like this will be 'Transfers subject to appropriate safeguards'. This is explained in Article 46 (in chapter V) of the GDPR here: https://gdpr-info.eu/art-46-gdpr/

This is a complicated document and if you are worried about it, wait to follow the lead of other, larger and obviously European businesses and organisations.

That, dear friends, is as heavy as it gets!

Remember, all these directives/guidelines are summarised from the ICO's instructions for data controllers in companies with departments and staff and managers.

When the same ICO describes getting ready for GDPR to 'micro-businesses' (less than ten employees) they boil it all down to eight steps, two of which are 'know the law is changing' and 'don't panic' and there is a link to that document on the landing page.

See you in the Facebook Group 😊