General Data Protection Regulation

What it means for Institute members

SUMMARY

The **General Data Protection Regulation** (**GDPR**) came into force on 25 May 2018.

Every business, charity or organisation which holds personal identifiable information must be fully compliant with the GDPR principles. This includes medical herbalists. GDPR applies to all Institute members within the EU and to all Institute members who work with anyone or process personal data of anyone who resides in the EU.

You will find information about GDPR
https://ico.org.uk/for-organisations/charity/

https://ico.org.uk/for-organisations/health/health-gdpr-faqs/

There are also some ICO podcasts and webinars which relate specifically to healthcare.
https://ico.org.uk/for-organisations/resources-and-support/webinars-and-podcasts/

The following guidance is to help you comply with GDPR. We aim to keep this as simple and straightforward as we can. Please note this is guidance and not legal opinion. If you have queries about anything to do with GDPR you should contact the ICO helpline or consult your own legal adviser.

What do Institute members need to know and do about GDPR?

All data that you have about patients, or customers if you have a retail outlet, is covered by GDPR. It also covers the data we hold on our suppliers and trades people who may do work for us. You must ensure you keep and process this data securely on an ongoing basis.

What action do you need to take to ensure ongoing compliance?

1. Understand and comply with the principles of data protection
2. Audit your data
3. Document your processes
4. Ensure security of the data you hold
5. Review and update your privacy policies
6. Put processes in place to maintain records for processing data including records of consent and retention of data
7. Have a plan for when people ask you about their personal data (Be prepared to respond to subject access requests)

1. Understanding and complying with the principles of data protection

Members need to ensure that their data processing activities are carried out in accordance with the Data Protection Principles set out in the GDPR.

Six Data Protection Principles
The six "Data Protection Principles" are that personal data must:

- be processed fairly, lawfully and transparently
- be collected and processed only for specified, explicit and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay
- not be kept for longer than is necessary for the purposes for which it is processed
- and be processed securely.

https://gdpr-info.eu/art-6-gdpr/

What constitutes data? What do you need to do with the data you process?

GDPR Article 4(1) provides the definition of personal data. It consists of several elements which all need to be present

1. I.e. personal data is any information
2. relating to
3. an identified or identifiable person;

The rest of GDPR Art 4(1) provides a further explanation.

There are two types of data, namely Personal Data and Sensitive Personal Data. As medical herbalists we process both – Sensitive Personal Data includes health information i.e. our patient medical records.

Personal data refers to any information relating to an identified or identifiable natural person, including but not limited to the following:

- First/last names
- Mailing addresses
- Email addresses
- Financial information
- Photos/videos
- Online identifiers (IP address, cookie strings, etc.)

(see Article 5 GDPR https://gdpr-info.eu/art-5-gdpr/)

If you process, i.e. collect, this type of information, you must:

- Comply with all six privacy principles (*see above*) and
- Satisfy at least one processing condition (*see below)*

Article 6(1) identifies six lawful grounds for processing personal data:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public interest task
- Legitimate interests

Art 6. https://gdpr-info.eu/art-6-gdpr/

This is expanded on page 9 below.

Sensitive Personal Data
(see Art 9, GDPR https://gdpr-info.eu/art-9-gdpr/)

Sensitive personal data under GDPR law is considered more sensitive and thus comes with greater protections and more stringent regulations.

Sensitive personal data includes the following:

- Health data
- Sex life/Sexual orientation
- Religious/Philosophical beliefs
- Political views
- Genetic data
- Trade union membership
- Racial or ethnic origin

If you collect this type of information, you must:

- Comply with all six privacy principles (see above) and
- Satisfy at least one sensitive personal data processing condition *(see Art. 9.2)*

There are ten processing conditions if you collect sensitive data; you must satisfy at least one of these if you collect sensitive personal data:

Sensitive Personal Data Processing Conditions

Any processing of sensitive personal data must satisfy at least one of the following conditions:

1. Have explicit consent of subject, unless reliance on consent is prohibited by EU/Member State law
2. Necessary for fulfilling obligations under employment, social security, social protection law or collective agreement

3. Necessary to protect vital interests of a data subject who is physically or legally incapable of giving consent
4. Processing is carried out by not-for-profit for members/former members and there is no third party disclosure
5. Data is manifestly made public by subject
6. Necessary for legal claims or courts acting in their judicial capacity
7. Necessary for reasons of substantial public interest under law, with safeguard measures in place
8. Necessary for medical purposes on the basis of law or contract with a healthcare professional
9. Necessary for public health interests such as cross-border threats
10. Necessary for archiving purposes in public interest, science or research

Data concerning health

Art.4(15)
"data concerning health" means personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status.

Art.9(2)(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

Accountability: you have a duty to show compliance with these principles

It is not enough to say that you are compliant – you must be able to prove it if asked. In order to do so, you will need to show that you have:

- robust, detailed data protection policies
- records of processing activities (e.g. data retention periods, transfers of personal data outside the EU, details of the recipients of personal data) This information can be requested at any time by the ICO. You will be required therefore to keep extensive internal records of data processing operations. To do this easily, create a data register containing information about all personal data processed by the organisation, including:
- the purposes for which the data is processed
- a description of the categories of data subjects and the categories of personal data, including if the data is sensitive personal data
- any transfer of the data outside the EEA
- the legal bases for processing the data
- the anticipated retention periods for the different categories of data
- the technical and organisational security measures used to safeguard the data.

What this means is that you will need to document what data you process, why you process and include the reasons for this in your privacy policy. Keep your policies and procedures in place and updated to ensure accuracy of the information you hold on an ongoing basis.

You cannot collect data and decide later how you will process it. You must ensure that, in relation to all processing activities by default, you process only the minimum amount of personal data necessary to achieve your lawful processing purposes.

Art. 5(2) requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

2. Audit the data you hold

First of all, **you need to conduct an audit of the data** you have. You need to know what data you have and you will use this audit to inform your policies and compliance processes.

You will need to know about, and keep a record, for all the data you hold:

- What data do you hold
- Where did it come from
- What is it used for
- Who has access to it/ who is it shared with
- What format is it in
- Who is responsible for it
- How long do you keep it
- The lawful basis for processing it/ the purpose for holding this data

The inventory at the end of this document will help you through this

process.

What constitutes personal data?
Any information related to a natural person or "Data Subject" that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

What is the difference between a data processor and a data controller?
A controller is the entity that determines the purposes, conditions and means of processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.
https://www.eugdpr.org/gdpr-faqs.html

It is likely that most of our members who are running their own herbal medicine businesses will be data controllers rather than data processors. However members may also be processors:

GDPR applies to all data
"The law protects personal data **regardless of the technology used for processing that data** – it's technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR."

https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

GDPR applies to all your patient health records and all personal data connected to anyone who interacts with your herbal practice; whether you store them on computer or on paper they are subject to GDPR.

3. Document your processes

Once you have audited the data you hold and process, you can use it to create a data register which documents your data processing procedures. Your data register should detail what data you have and how you will manage your data. You should review it periodically and ensure that the data is correct and up to date. Reminder: a data subject is any living person about whom you have any data.

Write down your thinking and reasoning. If you have got it wrong, and happen to be investigated, the ICO will see that you have tried to comply with the spirit of the legislation.

What is your lawful basis for processing the data?
You need to identify and document the lawful basis for processing all the data you hold. There are six possible lawful bases for processing:
consent, contract, legal obligation, vital interests, public task, legitimate interests

You must have a lawful basis for processing or you will be processing data

unlawfully. Your privacy policy should include the lawful basis (bases) for processing

data.

Below are the likely reasons for lawful processing for medical herbalists:

Consent
This must be a clear, affirmative act and for a specific purpose or purposes. It must be transparent and clear about why the data is being collected. If you are relying on consent as a lawful reason for processing, you should keep a record of where that consent can be found including when it was given, by whom, how and for what purpose(s) and keep a copy of the original document used at the time. A spreadsheet to record consent would be helpful.

You should use consent for e.g. newsletters or capturing data on e.g. websites. If you provide interested parties with a newsletter or market to them in any way, you may need to obtain fresh consent from them. There must be an active affirmative opt in, not an implied opt in and no pre-ticked boxes. You should be clear about what they are consenting to. You can either provide a list of opt-in tick boxes for each aspect of your marketing or you could provide a statement saying your newsletter contains articles, recipes, latest news, research, upcoming events and occasional offers with a single tick box. The former will require more work on your part to ensure you have consent for whatever you send to those on your list. You must have specific consent for each purpose so make sure your longer statement covers every eventuality. If you do not mention marketing, you cannot market to anyone who has not consented to it. You must allow for people to opt out at any time.

If you have an email list, it should contain an unsubscribe facility. You should also include a link to your privacy policy.

If someone withdraws consent, you need to take action as soon as possible, unless you have another lawful basis for processing.

You need **explicit consent** for processing sensitive data. This means you need to

give all patients a form to sign plus your privacy policy. If you have an online form for patients to complete before their appointment, your online form will need to take them to your privacy policy before they complete the form. If you email them a form, you will need to include your privacy policy and they will need to return the signed form to you, either by email (printed, signed and scanned) or to bring it with them when they come for their appointment. Keep this consent with their patient records.

We are unable to provide a consent form as these are specific to your business.
The ICO has complete guidance on consent including a checklist:
https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for- consultation-201703.pdf

To reiterate if you rely on consent as the lawful basis for processing any activities, you should review any consent mechanisms you have in place, to ensure that:

- data subjects are provided with a clear explanation of the processing to which they are consenting (clear plain language)
- the consent mechanism is genuinely of a voluntary and "opt-in" nature
- data subjects can withdraw their consent easily
- you do not rely on silence or inactivity to collect consent (i.e. pre-ticked boxes do not constitute valid consent)
- consent is not tied to other things e.g. terms and conditions

Contract
In essence, our patients are paying for our services and are therefore entering into a contract with us. Processing of sensitive data is necessary for you to be able to provide your services. You will be unable to fulfil your obligations to your patients unless you process their data i.e. take a medical history, write and dispense a prescription, provide appointments etc.

You would use contract as a means of processing if someone contacted you to ask about your services e.g. to make an appointment or to enquire about your fees or to ask if you might be able to help them. This falls under the steps that take place prior to entering into a contract, but to use this basis for processing you must ensure that the data subject has initiated and requested this. You cannot initiate this.

Legitimate interests
You can process data under the legitimate interests category if you have a relevant and appropriate relationship with the data subject. This could be a business relationship but you need to balance your legitimate interests with the data subject's interests.

It is not enough to just decide you are going to use legitimate interests, you will need to consider carefully if it is the appropriate data-processing basis for your business or

an aspect of your business. There is a clear procedure for deciding what data processing you can use under legitimate interests - a Legitimate Interests Assessment (LIA). This is a three-part test.

You will need to:

- identify a legitimate interest
- show that the processing is necessary to achieve it
- and balance it against the individual's interests, rights and freedoms.

The ICO breaks it down into the three stages:

1. **Purpose test:** are you pursuing a legitimate interest?

2. **Necessity test:** is the processing necessary for that purpose?

3. **Balancing test:** do the individual's interests override the legitimate interest?

It needs to be applied for each type of data processing that you do. You will find an example of a legitimate interest assessment here https://www.slaughterandmay.com/media/2535723/processing-of-personal-data-consent-and- legitimate-interests-under-the-gdpr.pdf

You may need to use the consent basis instead of legitimate interests if your data processing has the potential to harm the individual, or you are working with children's data.

When you conduct these tests, keep a record of the tests and results e.g. on a spreadsheet, so you will have evidence to back up your basis for using legitimate interests should it be needed. Make sure to identify your different uses of data in your privacy notice.

For further information on legitimate interests including a Legitimate Interests Assessment, see:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful- basis-for-processing/legitimate-interests/

Members are unlikely to use vital interests, public task or legal interest as a basis for processing data. However you should familiarise yourself with these in case you need to process data on one of these bases.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful- basis-for-processing/legal-obligation/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful- basis-for-processing/vital-interests/

The ICO has an interactive tool to help you decide the lawful bases for processing https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr- resources/lawful-basis-interactive-guidance-tool/

4. **Ensure security of the data you hold**

Under GDPR the primary requirement is that the controller must ensure the security of the personal data that it processes.

You need to make sure you keep the data you process secure.
You will need to assess, document and manage security risks.

You should lock your computer and devices when you are away from them and add suitable timeout and auto logout to your screensaver settings.

Your will need to document your storage arrangements to protect records and equipment in order to prevent loss, damage, theft or compromise of personal data.

Keeping data secure means measures such as:

- a lockable filing cabinet for paper records
- password protected access to electronic records
- configuring hardware to reduce vulnerabilities i.e. password protect
- controls over removable media e.g. memory sticks and mobile devices
- secure cloud storage within the EU
- encrypt backups, hard disks and other storage devices so they cannot be read if lost or stolen
- encrypt emails and email attachments
- install antivirus software and malware protection on your devices

You will need a procedure to inform data subjects if your data has been breached e.g. if a laptop computer, tablet or mobile phone has been lost or stolen.
You need to have a procedure that describes what you would do if....

If your website, email list or email marketing account gets hacked, be upfront about it and notify your website members / subscribers. Prevention is better than cure so make sure you use strong passwords.

Your security processes will also include how you dispose of records and equipment when they are no longer required.

If you need to you can secure access to your computer using a secure login key such as:

https://www.amazon.co.uk/dp/B01N6XNC01/ref=psdc_949408031_t2_B01M0DPK3K

https://www.vasco.com/products/

5. Review and update your privacy policies

If you haven't got one in place already, now is the time to do this.

GDPR is specific about what must be included in a privacy policy. Your privacy policy should be

- concise, transparent, intelligible and easily accessible
- written in clear and plain language, particularly if addressed to a child
- easily accessible and free of charge

Your privacy policy needs to include:

- Who you are
- What information is being collected How it is collected
- Why it is being collected (lawful bases) How it will be used
  Who it will be shared with
- How the person can access the data you process
  A statement about reviewing and updating the policy
- Where to complain or raise concerns including the details of the ICO
- Review and update statement

There are a number of free resources online which will generate a privacy policy for you. For instance Iubenda is an Italian company so is GDPR compliant where US based ones may not be. Iubenda will generate a privacy policy for you in about 10 minutes and it is free if you don't mind having Iubenda on your policy on your website or you can pay a small fee to remove the Iubenda mark. Thrive has a downloadable toolkit. We have provided these as examples and are not recommending any. You should confirm that any resource you use will enable you to be GDPR compliant. If in doubt, seek advice from the ICO and your legal adviser.

https://digital.com/blog/best-privacy-policy-generators/

http://jamieking.co.uk/blog/cyber-security/policies/free-sample-privacy-policy.php

https://www.iubenda.com/en/

https://wewillthrive.co.uk/resources/toolkits-templates/gdpr-build-your-own-privacy- notice

https://simply-docs.co.uk/Business_Documents

If you have a website you should have a Cookies policy and this should be included in your privacy policy. You should review your analytics tools to ensure they are GDPR compliant.

6. Put processes in place to maintain records for processing data including records of consent and retention of data

Create a system where you review your data processing regularly and ensure it is accurate and that you still have a lawful basis for processing it. You might for example include it with your accounting schedule. Ensure your retention procedure complies with your legitimate interest/legal concern for insurance purposes. (*see Balens advice below on p.16*)

7. Have a plan for when people ask you about their personal data

A key objective of the GDPR is to protect and strengthen the rights of data subjects.

You will need to be prepared to respond to Subject Access Requests. People have a right to know what data you process and for what purpose. They have a right to rectification (correction), erasure (to be forgotten) and data portability (to export their data).

Rights of data subjects
Right to information
Right of access
No fees
Right of rectification
Right of erasure (right to be forgotten)
Right to restrict processing
Right to information about the identities of third party
processors Right of data portability
Right to object to processing (including marketing and research purposes)

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

You have professional responsibilities including maintaining records for insurance purposes, which is a legitimate interest and legal concern and this may override some of these rights because of your legitimate interest. You will need to document this as a clear justification for processing. (*See information from Balens below*)

Hopefully you will only need to deal with requests to opt-out of your newsletters or email marketing lists. Most email providers make this easy and include a mandatory 1-click unsubscribe link for emails as well as a profile update function.

Data breaches

The term "data breach" is commonly used to refer to the scenario in which a third party gains unauthorised access to data, including personal data.

"Data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

In the event of a data breach, you must report the breach to the ICO without undue delay, and in any event within 72 hours of becoming aware of it. There is an exception where the data breach is unlikely to result in any harm to data subjects. The notification must include at least:

- a description of the data breach, including the numbers of data subjects affected and the categories of data affected;
- the name and contact details of the DPO (or other relevant point of contact);
- the likely consequences of the data breach; and
- any measures taken by the controller to remedy or mitigate the breach.

You must keep records of all data breaches, comprising the facts and effects of the breach and any remedial action taken.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation- gdpr/personal-data-breaches/

Do you need to register with the ICO?
You need to register if you process the information using computers or any system that can process the information automatically, including CCTV systems, digital cameras, smart phones, credit card machines, call logging and recording systems, clocking machines and audio-visual capture and storage systems.

If you only keep paper records, you will need to demonstrate that you do not receive communications from patients or other data subjects via telephone, voice mails, answering machines or email and other electronic means. If you ever write a letter to the patient or their doctor using a computer, you will need to register.

The fee is £40 or £35 if you pay by direct debit, and this fee is tax deductible.

https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for- controllers-20180221.pdf

Please contact the ICO if you have any questions.

Professional Indemnity Insurance and GDPR

The following information is provided by Balens, our bloc insurance scheme provider. If you have insured through another provider you need to contact them for advice about GDPR record keeping.

"Record Keeping and the GDPR"
We have received a number of requests from clients regarding record keeping in light of GDPR, and how long they should keep their client consultation notes / record cards for given the regulation notes that personal data should be kept for no longer than is necessary.

If you currently have a Balens Health Professionals Policy with us, underwritten by Zurich Insurance plc, it is a condition of your Insurance Policy to take and retain client records. The policy wording notes:

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

Record Keeping - Condition 14 c, on page 35

The Statute of Limitation in the UK (i.e. time when an individual is able to bring a claim) is 6 years for certain injury claim situations, or 6 years after the individual reaches the age of majority in the case of minors. However, these 6 years start from the date that the injury was discovered, not from the time that the alleged incident that caused it occurred. There are also instances, for example if treating a vulnerable client, where the statute may be overturned. Your records are your best line of defence in any claim situation hence the need to keep these for at least 7 years. It will be for you to determine, in view of your own client base, whether you choose to keep the records for longer than the 7 years noted in the policy wording, and then note this in your Privacy Notice for your clients.

There are provisions under the GDPR with regards to keeping records to defend yourself in a claim situation (https://ico.org.uk/for-organisations/guide-to-the-general- data-protection-regulation-gdpr/individual-rights/right-to-erasure/ When can I refuse to comply with the right of erasure), which clearly give you the right to hold your client records to comply with your insurance Terms and Conditions, should your client make a request for them to be deleted under their Right of Erasure."

Source: Balens 21st April 2018

Art.9(2)(f) The processing is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity

If you have any questions, we respectfully request that members contact the ICO. They are the regulators and they will give you definitive advice.

N.B. This guidance is not legal opinion. If you have queries about anything to do with GDPR you should contact the ICO helpline or consult your own legal adviser. The Institute bears no responsibility for loss or damage arising from use of this guidance.

https://ico.org.uk/global/contact-us/helpline/ Tel: **0303 123 1113**

Further information on the ICO website:
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/making- data-protection-your-business-campaign-launched-to-help-micro-businesses-prepare- for-the-new-data-protection-law/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation- gdpr/

https://ico.org.uk/for-organisations/business/