bacpac

GDPR for counsellors and therapists

What does the General Data Protection Regulation update mean for you?

What does the General Data Protection Regulation update mean for you?

There's been a lot of coverage in the media recently about the new EU ruling on data protection - the GDPR (General Data Protection Regulation), and as therapists and counsellors you might well be wondering what all the fuss is about and what it means for you.

Well, as a therapist or counsellor, you are classified under the GDPR as a 'data controller' and there are some requirements that you will need to meet.

We at **bacpac** thought we'd help shed a bit of light on the subject with this short ebook.

The contents of this ebook have been created based on information provided by the Information Commissioner's Office, licensed under the **Open Government Licence**. You can read more about the GDPR on the **Information Commissioner's Office (ICO) website**.

Today, local regulations around privacy and electronic communication differ across European countries. The GDPR (General Data Protection Regulation) is a new EU Privacy Law created to make sure the laws across European countries are consistent. The new law will be enforceable from May 25, 2018 with pretty serious penalties for those not attempting to comply.

Who does it affect?

The new law applies to both controllers and processors.

A controller determines the purposes and means of processing personal data. As a therapist or counsellor, you're classed as a controller.

A processor is responsible for processing personal data on behalf of a controller. That's us at **bacpac** - we look after your client data.

Key terms

Demystifying a few key terms that are used in the documentation seems a good place to start. Here's a list of six that we think are really useful to know...

Data Controller
A person who determines both what and how any personal data is used (eg therapist, counsellors or a group thereof)

Data Processor
A person/organisation who processes data on behalf of a data controller (that's us at **bacpac** - we look after your client data)

Data subject
A person who is the subject of personal data (eg your clients)

Processing
Any handling of data - holding, recording, sending, analysing using and destroying it

DPA
Data Protection Act

Personal Data
Any data relating to a living person or 'data subject', that can be used to directly or indirectly identify the person

About the author

Martin Davies is the commercial product owner for bacpac. He works closely with the product development team at Mayden, whose focus is on continually developing and managing a system that really works for professionals in private practice; one that is simple, portable and secure, and which reduces the amount of time therapists spend on admin.

Steps you can take now to prepare for the GDPR

Lots of the GDPR's main concepts are similar to those in the current Data Protection Act, so if you're complying with the current law you have a good starting point to build from.

There are some new elements though, along with some enhancements to the current law, so there are some things you will need to do differently.

Check out the following steps to prepare for the GDPR.

1 Awareness

Make sure that decision makers and key people in your organisation know the law is changing. It's important that they understand the impact the GDPR will have and are aware of things within your organisation that could cause compliance problems under the GDPR.

Does your organisation have a risk register? If so, start by looking there. Implementing the GDPR could be quite demanding on your resources and you're likely to find complying in time quite a challenge if you leave your preparations to the last moment.

2

Information you hold

Take an audit of the personal data you hold, where it came from and who you share it with.

The GDPR requires you to keep records of your data processing activities.

For example, if you have inaccurate personal data about an individual and you have shared it with another organisation, you'll have to tell the other organisation about the inaccuracy so it can correct its own records. Unless you know exactly what personal data you hold, where it came from and who you share it with, you won't be able to do this.

Documenting this info will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

3

Communicating privacy information

You should review your current privacy notices and put a plan in place for making any changes necessary for GDPR in time for 25 May 2018.

Currently, when you collect personal data you have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice.

Under the GDPR there are some additional things you need to share with people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

4

Individuals' rights

Check your procedures to make sure they cover all the rights that individuals have, including how you'll delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling

On the whole, the rights individuals have under the GDPR are the same as those under the DPA but with some enhancements. If you're geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy.

This is a good time to check your procedures and to work out how you would respond if someone asked to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who would make the decisions about deletion?

The right to data portability is new. It only applies:

- to personal data an individual has provided to a controller
- where the processing is based on the individual's consent or for the performance of a contract when processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured, commonly used, machine readable form and provide the information free of charge.

5

Subject access requests

Update your procedures and plan how you'll handle requests under the GDPR:

- in most cases you will not be able to charge for complying with a request
- you'll have a month to comply, rather than the current 40 days
- you can refuse or charge for requests that are manifestly unfounded or excessive

if you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy, and you must do this within one month, without delay

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. Consider developing systems that allow individuals to access their information easily online.

6

Consent

Review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

Read the **detailed guidance** the ICO has published on consent under the GDPR, and use their consent checklist to review your practices.

Consent must be freely given as well as specific, informed and unambiguous. There must be a positive opt in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you should offer simple ways for people to withdraw consent.

You're not required to automatically update your existing DPA consents, but if you're relying solely on individuals giving consent, you'll need to make sure that it meets GDPR standards in that it's detailed but clear, prominent, obviously an opt in, well documented and easy for the client to withdraw consent.

7

Children

Start thinking now about whether you need to put systems in place to verify individuals' ages and obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children's personal data. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully.

The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'.

This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

8

Data breaches

Make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Under the GDPR, all organisations have a duty to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

9

Data protection by design and Data Protection Impact Assessments

So what are 'protection by design' and 'Data Protection Impact Assessments'?

Put simply, 'protection by design' is a practice that ensures that privacy and data protection compliance are always a high priority in all the big projects that you undertake within your own practice - installing a new record keeping system for example.

DPIAs are a tool which can help you identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy.

It has always been good practice to adopt a 'protection by design' approach and to carry out a Privacy Impact Assessment (PIA) as part of this. But the GDPR makes protection by design a legal requirement, under the term 'data protection by design and by default'.

It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed
- where a profiling operation is likely to significantly affect individuals
- where there is processing on a large scale of the special categories of data

If a DPIA indicates that the data processing is high risk, and you can't sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Start to assess the situations where it might be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

Familiarise yourself with the **guidance the ICO has produced on PIAs** as well as guidance from the **Article 29 Working Party**, and work out how you can implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.

You can be sure your data is safe with us

bacpac® is a comprehensive yet simple and versatile client management system for counsellors and therapists working in private practice. With a dedicated and friendly support team on hand to help with any queries, bacpac could be the edge you need.

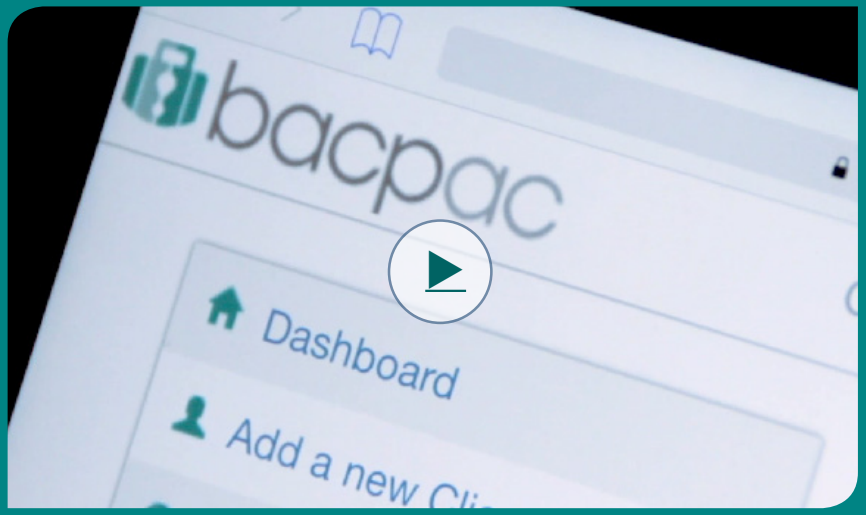
The security of your client information is our foremost concern

Mayden, the company behind **bacpac** has over a decade of experience handling confidential patient data. We have reviewed our procedures and policies in the light of the GDPR and the necessary steps to comply with the new measures.

Mayden is ISO 27001:2013 accredited. This internationally recognised information security management standard ensures that a business has stringent processes in place to ensure data confidentiality and to identify, manage and reduce risks to information security. Find out more **here**.

Find out more

Hear what other counsellors have to say about **bacpac** by watching our short testimonial **video.**



And why not join us for a free webinar to find out more about bacpac? Click **here** to reserve a spot.

martin.davies@mayden.co.uk