What is the General Data Protection Regulation? (GDPR)

The GDPR is a regulation by which the European Parliament, the Council of the European Union and the European Commission intended to strengthen and unify data protection for all individuals within the European Union, aiming to give control back to citizens and residents over the way their personal data is used.

The GDPR came into effect from 25th May 2018.

Taking data security and privacy seriously

At CalmBrain®, we take data security and privacy extremely seriously and believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights, and as such we are committed to maintaining compliance with the GDPR.

We have undertaken a GDPR audit and worked to action any points highlighted from this to ensure data handling best practice is followed.

We also have key policies that cover, in addition to this document, how we handle and manage data on behalf of our customers. Links to the policies can be found below: -

- Terms & Conditions
- Privacy Policy

There are additionally some FAQs that follow below:

Thank you for trusting us with your business and please be assured that we will always take the security and privacy of our customers data very seriously.

Sincerely,

The CalmBrain Team.

CalmBrain®
Regulating Emotions & Behaviour

Frequently Asked Questions

Are you registered with the Information Commissioners Office (ICO)?

We are registered, and are currently awaiting our registration number.

What legal, regulatory and contractual requirements do you operate under?

CalmBrain complies with all legal, regulatory and contractual requirements related to information security and adopts UK law guidelines, industry standards and best practice for information security.

Is CalmBrain a data processor or a data controller?

For our Customers, we act as a data processor, meaning that we process your personal data on your behalf, in accordance with our Terms & Conditions.

The following reflects the different groups and their role within the end to end data process for CalmBrain:

Employee/Student/Child/Caregiver/HealthCare Professional

DATA SUBJECT

Customer/School

DATA CONTROLLER

CalmBrain

DATA PROCESSOR

Have you appointed a Data Protection Officer (DPO)?

Yes, our DPO is our Chief Technical Officer, Graham Iles.

Will I be notified in the case of a breach?

Under the GDPR, CalmBrain is required to report data breaches to the ICO within 72 hours. As part of our information security incident management procedure, appropriate communications will be made, including notifications to all affected parties.

How do you handle subject access requests (SAR)?

CalmBrain acts as a Data Processor on behalf of its Customers so we are not able to process SARs on your behalf. If we receive a SAR from one of your employees/students we will forward the request to you.

How do you process data portability requests?

CalmBrain acts as a Data Processor on behalf of its Customers so we are not able to process data portability requests on your behalf. We provide you with tools inside CalmBrain to extract information in commonly used file formats.

Do you share my data with anyone?

CalmBrain has a strict policy of not sharing any information about any customer, user or data subject with anyone outside the organisation. CalmBrain will not share data with third parties unless explicit instruction is given by the customer in question.

Where is my data stored?

CalmBrain stores data on secure database servers held within the Microsoft Azure cloud services ecosystem. Microsoft are an internationally recognised and leading provider of cloud services. They are trusted and used by many of the leading UK and Global organisations. Physical access to Microsoft servers is strictly controlled and limited to authorised personnel in order to maintain their servers.

How have you documented the Personal Data you hold?

CalmBrain has completed a full company wide information classification assessment; this allows us to understand the data in every part of our business (both our own data and that entrusted to us), the highest level of protection required for each of these data sets and how we can further implement controls to reduce the likelihood of an incident impacting these assets in the future.

What training do your staff go through?

CalmBrain develops and provides ongoing security awareness training for all staff and actively promotes the key principles of information security.

How do you comply the requirements of the GDPR principles?

There are 6 principles within the GDPR framework, these are:

1. **Lawfulness, fairness and transparency**

   We process any personal data we collect in a fair, lawful and transparent manner; and in accordance with individuals' rights.

As a Customer of CalmBrain we will only process the personal data you enter into the system in accordance with our Terms & Conditions.

2. **Purpose limitations**

   We will only collect personal data for specified, explicit and legitimate purposes. Data we collect will not be used for any other purposes other than what you as the data subject(s) has been made aware of.

   As a Customer of CalmBrain we will only process the personal data you enter into the system in accordance with our Terms & Conditions.

3. **Data minimisation**

   We will only collect personal data that is needed, adequate and relevant for the specific purpose. As a Customer of CalmBrain you are responsible for ensuring that the data you hold about any users is limited to what is needed, adequate and relevant for the specific purpose.

4. **Accuracy**

   To the best of our ability we will ensure that any personal data we collect is accurate, kept up to date and correct.

   As a Customer of CalmBrain you are responsible for ensuring that the data entered into the system about any user is accurate and kept up to date. Our systems are designed to maintain a high level of integrity, meaning that your data will remain as entered and unchanged.

5. **Storage limitations**

   As a Customer of CalmBrain you are responsible for ensuring that personal data entered into your system is removed when no longer needed. If you choose to close your account we will securely anonymise all personal data held in the system on your behalf in accordance with our Privacy Policy.

6. **Integrity and confidentiality**

   We will process all personal data we collect in a manner that protects it against unwanted modification, disclosure or unlawful processing.

   We take a risk-based approach to ensure that our systems have the appropriate technical and organisational controls to safeguard the integrity and confidentiality of all personal data.