What is the General Data Protection Regulation? (GDPR)

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

The GDPR comes into effect from 25th May 2018.

Taking data security and privacy seriously

At breathe, 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, as such we are committed to maintaining compliance with the GDPR.

Under any compliance regime, it is easy to state compliance but much harder to prove. To this end, we have taken the decision to implement an information security management system which is certified to the requirements of ISO27001:2013.

By gaining certification to ISO27001:2013, breathe can ensure that the appropriate controls for the management of information are in place and that we are working to meet our legal and regulatory requirements, including those outlined in the GDPR.

By working with a highly respected data security consultancy, we aim to achieve ISO27001:2013 certification within the first half of 2018.

To provide you with more information about the actions we are taking please see the documents below:

- Information Security Management System
- Policies and Procedures
- Frequently Asked Questions

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

Jonathan Richards
CEO, breathe

Information Security Management System (ISMS)

Who is the legal entity behind breathe?

Breathe is the trading name of Centurion Management Systems Ltd, a company registered in England under company number 3020608.

How do you ensure that personal data is handled appropriately?

breathe operates and maintains an Information Security Management System (ISMS) to control its information assets appropriately. Certification to the information security standard ISO 27001 will be achieved in the first half of 2018.

We implement human, organisational and technological security controls to protect our information assets (including personal data) from unauthorised access, unwanted disclosure, modification, theft / loss, denial of service attacks, or any other threat.

breathe has implemented and applies internal policies and procedures that support the ISMS. As part of a management system these will be independently audited by a certification body at least annually and by external security specialists.

breathe uses a scalable cloud computing platform with high availability and dependability.

To achieve end-to-end security and end-to-end privacy all services are built in accordance with security best practices, privacy by design requirements and appropriate security controls.

How have you documented the Personal Data you hold?

breathe 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.

How do you manage risks and incidents relating to information assets?

breathe uses a formal information security risk management framework to identify and manage known or potential risks to the information assets within our business. Our risk management framework analyses each information asset against the possible loss of confidentiality, integrity and availability and defines appropriate controls.

We operate a formal incident management process to identify, contain and recover from a security incident should one occur and uses this process to help prevent reoccurrence.

What training do your staff go through?

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

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

breathe 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.

Policies & procedures

breathe has developed policies and procedures based on industry and vendor best practices to protect the information assets it keeps for our customers, partners and our own information assets. The communications and operations management is planned for and deployed with regard to the security of breathe information assets and the operations of the whole information processing environment.

Our policy and procedures set standards for our information security controls, some examples being

- Information security policy
- Clear desk and clear screen policy
- Asset management policy
- Cryptographic policy
- Access control policy
- Acceptable use policy
- Mobile computing policy
- Incident management procedure
- Information classification procedures
- Risk management procedure
- Internal audit procedure
- Document and records control procedure
- Corrective actions procedure
- Preventive actions procedure

Each policy and procedure supports the required controls as set out by the ISO27001 standard Statement of Applicability and how breathe manages its information.

Where can I find your Privacy Policy?

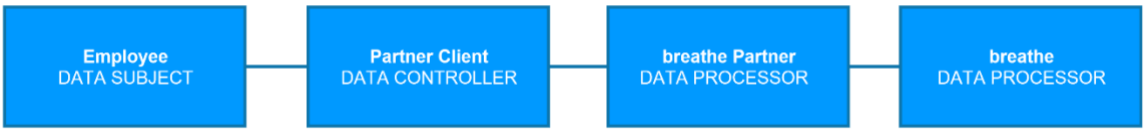
For further information on how we process (collect, store, share and handle) your data is available in our company Privacy Policy.

Frequently Asked Questions

Is breathe 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 the End User License Agreement.

For our Partners, we act as a data processor meaning that we process your clients' personal data in accordance with the Partner Agreement and the End User License Agreement.



Have you appointed a Data Protection Officer (DPO)?

Yes, our DPO is our Chief Executive Officer, Jonathan Richards.

How do you comply the requirements of the GDPR principles?

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

Lawfulness, fairness and transparency

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

As a Customer of breathe we will only process the personal data you enter into the system in accordance with the End User License Agreement.

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 breathe we will only process personal data you enter into the system for the purpose of providing you our service and in accordance with the End User License Agreement

Data minimisation

We will only collect personal data that is needed, adequate and relevant for the specific purpose.

As a Customer of breathe you are responsible for ensuring that the data you hold about your employees is limited to what is needed, adequate and relevant for the specific purpose.

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 breathe you are responsible for ensuring that the data entered into the system about your employees 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.

Storage limitations

We will only keep personal data we collect for as long as it is needed, in addition, you have the right to request erasure of your individual data.

As a Customer of breathe 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 delete all personal data held in the system on your behalf.

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.

Do you perform Privacy Impact Assessments? (PIA's)

We perform periodic risk assessments in accordance with the ISO27001:2013 standard which addresses the confidentiality, integrity and availability requirements of any personal data handled by breathe.

Our risk assessment methodology includes a full assessment of what data we hold, where this information is located, the risks involved with processing this information and the controls necessary to address the associated risks.

Will I be notified in the case of a breach?

Under the GDPR, breathe 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)?

breathe act 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 we will forward the request to you.

How do you process data portability requests?

breathe act 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 breathe to extract information in commonly used file formats.

How do you ensure you meet with the privacy by design requirements?

As part of our information security management system, we have implemented system development principles to ensure that whenever we develop or introduce new systems, privacy and security requirements are considered at every stage.

Where is my data stored?

We use Amazon Web Services (AWS) located in Ireland to store our databases and production environment, these services are supported by our disaster recovery site in Germany. This means we never store your data, or indeed any of our backups, outside the EU.

If you have any further questions regarding the breathe infrastructure you can find more information in our Security and Reliability Whitepaper.