breatheHR security, reliability and GDPR

Contact us: Tel 01403 288700 breathehr.com @breatheHR

General Data Protection Regulations (September update)

You may be aware that in May 2018 the new General Data Protection Regulations (GDPR) legislation comes into force. The GDPR imposes new rules on organisations who offer goods and services to people in the European Union (EU), or who collect and analyse data tied to EU residents.

Taking data security seriously
At breathe, we have always taken 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 GDPR compliance when enforcement begins May 25, 2018.

Our aim has always been to provide you with the highest level of data security and as such we constantly review and reinforce our security practices. An example of this was when we moved our data hosting to Amazon Web Services (AWS) to ensure your data was held in the most secure hosting environment, backed up by their ISO27001 accreditation.

One step further
Under any compliance regime, it is easy to state compliance but much harder to prove it. To this end, we have taken the decision to achieve our own ISO27001 accreditation that will sit alongside the AWS accreditation. We are currently selecting an implementation partner and work will start in September.

Those of you who are familiar with both GDPR and ISO27001 will know that there isn't a direct fit but both aim for high levels of data security and privacy. My brief to our implementation partner is to put in place an ISO27001 system that ensures compliance with both sets of regulations.

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

Jonathan Richards CEO, breatheHR

Security and Reliability

"How safe is my data?"

This is a perfectly reasonable question. We're not only talking about data that is very personal, but in many cases very sensitive. If you were to put this information into a system that was not secure, and run the risk of this data being lost or even maliciously intercepted by someone, then your job would be on the line. Even worse, you might be opening up your organisation to legal action. So first and foremost please rest assured - we understand how big of a deal it is. Data protection and security is very much our first priority and the security of your data governs every development decision we make. We take no steps back when it comes to security. We not only believe that we have a legal responsibility to ensure the safety of your data, but also a moral one. We protect your data because frankly it's the right thing to do. This document outlines the steps we take to ensure that you can use breatheHR with confidence, and the processes we put in place to ensure this confidence is well placed.

From your computer to us

The journey of your data starts with yourself. We do not allow single sign on from other systems because we believe people should have to maintain a unique password for breatheHR. Convenience does not trump security in our book. So every user has to enter a password, and we recommend that password is long and complicated. This bit is down to you I'm afraid, but we recommend you ask your users, and specifically your HR users, to test their passwords against a recognised and reputable security site such as https://howsecureismypassword.net/ . Your username and password information is encrypted by us in the database. Once you've typed the data into breatheHR, that's where we start to help with security. Whilst we do not encrypt all data, your security is immediately encrypted in the database. No-one can access your password. No-one.

Browser encryption

Long version: Browser sessions describe how your browser talks to our servers. this is the first step in security, with data flying back and forth. These sessions are encrypted with industry standard SSL, utilising a 2048 length private key, way beyond what is normal industry standard. Our SSL certificates are signed with a SHA-256with RSA algorithm. We only accept connections from browsers with a strong cipher suite, and will not allow weak encryption for SSL Sessions. We are not affected by the Debian weak encryption key problem. We support the latest TLS 1.2 protocols. We are not vulnerable to POODLE attacks, or HEARTBLEED.

Short version: Our technical people stay on top of the latest security news, and everything is encrypted in transport to the latest standards. Given that the estimated time to hack encryption of this type is significantly longer than the age of the universe then we're comfortable that your data is safe on its way to us.

Physical security of Data

Long version: Your data is all located on Amazon AWS instances in the EU, and never leaves the EU. Amazon is ISO 27001 certified. We are registered with the information commissioner's office, and comply with all data protection regulations. Your data is stored in a secure data centre, with multiple levels of security including crash barriers, complete CCTV coverage, motion sensors, trip lights, state of the art alarms, and roving guards. The centre has reinforced access doors, digital key storage systems, multiple pin entry systems, electronic and physical access logging, and an array of other physical security measures designed to stop someone getting into the building. Even if they do, the servers are all physically and separately secured. The servers are all protected with a digital gateway which means multiple layers of security requiring different levels of authorisation.

Short version: Our servers are protected from access by everyone. As the product founder, even I am not allowed physical access to the servers.

Server security

Long version: We do quite a lot to prevent hackers from obtaining access to the server, and indeed to prevent our own staff and vendors from doing things they shouldn't. the first is that we are regularly penetration tested by a CREST accredited recognised 3rd party auditor. We use the Security Bureau in Brighton (www.thesecuritybureau.com), and were last audited at the end of 2015. The result was uniformly positive, with the tester finding "there was no way of accessing the application without valid security credentials". In other words, no username and password, then you're not getting in. We achieve this result by: 1. Ensuring that the servers are locked down to access only by SSH private / public key combinations 2. Making sure all servers are kept up to date with security patches and updates 3. Permitting access to only those people that need access and even then only to the level they need it. 4. Regularly updating a list of those individuals who can access the servers, and ensuring the reason for them doing so is still valid 5. Logging every access to the server and reviewing those logs regularly.

Short version: Our machines are kept up to date, patched regularly and can only be accessed directly from specific people in specific locations. The only people who can access the servers are the people that need to access the servers in order to make breatheHR happen.

Application security

Long version: breatheHR has been built with the latest version of Ruby on Rails, following well documented best practices for secure application development. The application does not produce leak error or process information, handles all user input in a secure manner, takes steps to prevent escalation of permission attacks through missing function-level access control. We also code to avoid CSRF attacks, session attacks, cross site scripting, SQL injection, and many other nasty little tricks that people play. We're also paranoid about our people, so the applications stops our support staff from accessing your data unless you give them

specific consent to do so. Sales and marketing staff have access to general metrics in the system but no access whatsoever to your employee data. Developers are required to develop in a test environment only, and will only access account data as part of second line support - again with client informed consent only. All security information, including session information, is encrypted. All backups are encrypted both in storage and transport.

Short version: As well as professional auditing we also invite our client's IT teams to have a go at hacking the application. If they can break in (and prove it), we will fix the problem immediately and you will not pay for breatheHR, ever. A few have tried. They are still paying us. We do everything we can do prevent both unauthorised access from people outside breatheHR, and unauthorised access of your account from within breatheHR.

Availability

Long version: Our availability for the last calendar year was 99.95%, which includes time for all new releases and maintenance etc. We plan to aim even higher this year. We achieve this in a few ways.

1. **Load-balancing** – We now run a multi instance application, which means breatheHR is simultaneously running on multiple servers. If we lose a server, the application stays up.

2. **Automated scaling** – If the application thinks it needs more power in order to continue to deliver high performance, it will simply add another server to itself. When the demand goes down it will turn that server off. Which means breatheHR will be available when you need it.

3. **Rolling updates** - Updates are rolled out one server instance at a time. This means that as one server is being updated, you will be automatically re-routed to another server. This means most updates can be done without disturbing clients or taking the system down.

4. **Multi Availability zone** – although all our servers are in the EU for data protection reasons, they are housed at multiple secure sites, so even in the event of an entire site going down, breatheHR will continue to remain operational.

5. **Backups:** Backups are taken every 5 minutes and kept for months. These are all kept on a secure amazon S3 encrypted bucket. By the way, we've never had to restore a backup, although we do practice.

6. **Development best practice:** all our development code is checked by multiple developers in a laboratory environment before being pushed to a staging environment. At this point it is checked yet again by front end users. This way we aim to catch development issues long before they hit the live server. Code is checked for security first, performance second, and only then functionality. We take looking after your data very seriously.

Short version: We do everything we realistically can to ensure breatheHR will be there when you need it. On the extremely rare occasions where this isn't the case our development team will be all over the problem and will keep you informed.

Office security

Long version: To break into our offices someone would have to go through multiple locked doors, and override a modern alarm system. We all work from laptops and access the data kept safe and secure in the data centre. Your data is not kept on any servers in our office, and not kept on any laptops. If you send us data by email, we will immediately delete it and explain it to you why this is a bad idea. If we do have to get data from you, we will use a secure mechanism and ensure all files are encrypted.

Short version: Worried about someone breaking into the breatheHR offices? Don't be. They can't access your data even if they sit at our desks.

Short Questions and Answers

"Where do you keep my data?"
The data is kept in a secure data centre in the EU and your data will never ever leave the EU. It's not kept on any of our laptops or in our office.

"Is breatheHR protected with SSL?"
Absolutely.

"What about data encryption"
Everything is encrypted in transport, and then your security data is encrypted in the database. 256 bit encryption algorithms, 2048 character keys.

"Do you allow everyone in your team to access our data?"
No. Only people with a valid reason can access your data, and even then its at your say so.

"Would you sell our data to other companies?"
No, despite the fact that it's illegal, it would be completely wrong. No, we would never do this.

"Do you backup our data?"
Throughout the day, and every day, including weekends. Then it gets put somewhere safe and secure just in case. Even fewer people can access the backups than can access the server.

"Do you get penetration tested?"
Yes, and we view it as a positive thing. The result of the last test demonstrated it was impossible to access a breatheHR account without valid credentials.

"What if the internet isn't quick enough?"
breatheHR uses AWS's 2GB internet pipe. So any problems with speed won't be at our end. You should be able to access breatheHR happily through a 3G phone signal. If your internet connection is fast enough to browse the web, it's fast enough to use breatheHR

"What if the entire internet goes down?"
In that situation breatheHR would not be accessible, but then I would think the loss of your access to the internet / email / communication would be more of a worry for you. In that event we would safeguard your data and wait for everything to blow over. In fact, breatheHR is likely to stay up long after your other systems have gone down as we have redundancy built in at several levels.

"What if the server crashes?"
breatheHR exists on a load balanced auto scaling environment. This means we tell it we want X servers running all the time. If 1 goes gown, it fires up another one. You won't even notice.

"How reliable is breatheHR?"

In a word, very. Our redundant infrastructure design, the robust security and 24/7 monitoring all mean that the system is incredibly reliable.

"What if I have any other worries?"

I hope this document has mitigated your concerns about security, and more than anything else I hope I have managed to convey that I take the security of your information very seriously and that it is a personal passion of mine.

Gareth Burrows
Chief Technical Officer, breatheHR