citrusHR

Online Security

We understand that we store information on our website about your employees which is highly sensitive, and we take protecting that very seriously. In fact, we believe that the sensitive data that we store is more secure on our website than it is in the traditional physical filing cabinets in which we have all stored this data historically.

The new GDPR law requires companies to store personal information as securely as possible, and we believe that we do, and are totally committed to continue to do, that to a very high standard.

Here is a brief summary of how we look after your data:

- **We encrypt the data** transferred between your PC or device and our server.
- **We encrypt the data** stored on our servers.
- Our main server is based in the UK in a secure location with 24x365 security equipment and staff. We do not disclose this location. Major banks use the same secure location.
- **We back up our data every day** to two additional, separate locations, one in the UK and the other elsewhere in the EU, and both with the same high levels of physical security- and both still store only encrypted data.
- **We restrict access** to your data only to those staff who absolutely need to have it—and we conduct thorough personal background reference checks on all staff who have access to customer data.
- **We conduct multiple electronic checks** on our data every day.
- We pay a **specialist cyber security consultancy** to try to test our system for any potential vulnerabilities at least once every year, and to advise us on any new measures we can take to further strengthen our security.
- **We monitor the latest security techniques** used by other leading software companies to make sure that we stay on top of all new approaches.

Our focus is both on maintaining continuous client access to their information and on preventing theft of that information by unauthorised parties (both criminals and "nosy staff" seeking information about their colleagues).

Data Backup

We back up our client data every day to a server at a separate physical location from our core web host. This provides assurance that in the event of a problem at one location, for example fire or flood, we will not only be able to restore the data but also provide continuous service to clients. We comply with EU regulations for storing personal information, and ensure that both the main server and the backup are located within the UK. This also has the advantage of making it faster to serve information to client requests.

Prevention of Data Theft

Data can be stolen from a location where it resides or from the journey from our server to a client computer. We therefore take steps to secure both.

Physical security

Our main and both backup servers are located in highly secure locations.

Risk of theft through hacking

The main risk that many people worry about is "hacking." Hackers could attempt to break into our servers and steal files without logging into our software, or log in and steal files once inside, or steal files while they are travelling between our clients' computers and our servers. We deal with each threat separately:

Server protection

Our hosting company provide both hardware and software firewalls to protect our servers. These are scanned permanently by automated tools to ensure they are running securely. Our host reviews its procedures regularly in order to keep up with the latest security measures. Its other hosting clients include both large private organisations and governmental health and security departments with highly sensitive data; some of these clients regularly test our hosting company's procedures to ensure they remain robust. Our data benefits from the same levels of security as the hosting company's other clients.

Software protection:

Our software requires users to log in using their username and password. We use industry standard authentication software developed by Microsoft for this.

We recommend that users change their passwords frequently and keep them confidential.

We support Two-Factor Authentication, which is considerably more secure than passwords which can often be guessed- and we highly recommend that you use it.

Our software automatically logs users out after 20 minutes of inaction to minimise the risk that a passer-by can jump on to a device logged onto our software and make unauthorised use of it.

Human Error

We believe that the greatest practical risk to the data our clients store with us is human error—the most likely issues being that an employee is logged in to our system and leaves their desk for a while, leaving scope for someone else at the premises to see information about that client which it should not see. More likely than that is that a member of staff either gives their password to a colleague, or writes it down and leaves it in a place where others can see it. We have quite literally seen companies where people have written their password on a yellow sticky note attached to their computer screen!

We urge all our clients to be vigilant, both with staff training and active monitoring to help prevent this sort of human error.