

Mobile Office is registered under the Data Protection Act 1998 (ref: ZA159896)

Web and information security for our website – www.mobileoffice.guru

- Our website is hosted at the Rackspace London data center <https://www.rackspace.com/about/datacenters>
- Running on Rackspace Cloud server & Cloud Database. Managed hosting.
- Linux Firewall behind Rackspace Load Balancer
- All logins to Rocketspark Dashboard and site edits are done over a secure HTTPS connection.
- All access to servers is via secure SSH public/private key encryption by Rocketspark technicians
- Backups are run daily, locally and offsite to our Rackspace Australia server with the same security policies.
- OS is Linux Centos
- Security patches and updates are run regularly.
- All file uploads to the server and code is QA tested internally.
- User file uploads are put in a non-executable location on the server.

Web and information security details for competence assessment and risk assessment forms

All raw assessment data is hosted on Amazon's AWS service:

Our assessments and all of the raw assessment data that we collect are hosted by Typeform who use Amazon's AWS servers based in Virginia (US). However, we can continue to use Typeform (i.e. AWS) to transfer data from the EU to USA without altering the architecture, and in compliance with present EU law (post the ECJ Safe Harbour ruling). This is possible because AWS has already obtained approval from EU data protection authorities (Article 29 Working Party) to enable transfer of personal data outside Europe, including to the USA. This means Typeform can continue to run global operations using AWS in full compliance with the current EU Data Protection Directive.

You can find further information at:

<http://aws.amazon.com/security/>

- <http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html>

- <https://blogs.aws.amazon.com/security/post/Tx3QAALRNBIK9K1/Customer-Update-AWS-and-EU-Safe-Harbor>

- <http://aws.amazon.com/compliance/eu-data-protection/>

- <https://aws.amazon.com/compliance/data-privacy-faq/>

Web and information security details for competence assessment certificates and risk assessment reports which we store for you using Tresorit cloud storage (www.tresorit.com)

Tresorit uses Microsoft Azure servers that operate in Ireland and the Netherlands and your data never leaves the EU. <https://azure.microsoft.com/en-gb/support/trust-center/>

Tresorit uses client-side 256-bit encryption (end-to-end encryption) and zero-knowledge security technology. This means that no-one has the encryption keys other than us - Mobile Office and you, our client – not even Tresorit administrators can access your data.

To learn more about Tresorit's high levels of security follow this link: <https://tresorit.com/security>

Secondary backup of records

If requested by clients we also maintain a second backup of our clients' files on a 256-bit encrypted (password protected) external hard drive which is securely stored at Mobile Offices's registered company address in the UK. This hard-drive is kept offline as a default and is only online when backing up data.

Our data protection policy

Mobile Office Ltd. is committed to preserving our clients' privacy and information security. We will never pass on our client's details to any third party without your specific agreement and knowledge. The information management sites which we use maintain high levels of backup and security. If you have any more specific questions or concerns please get in touch at hello@mobileoffice.guru