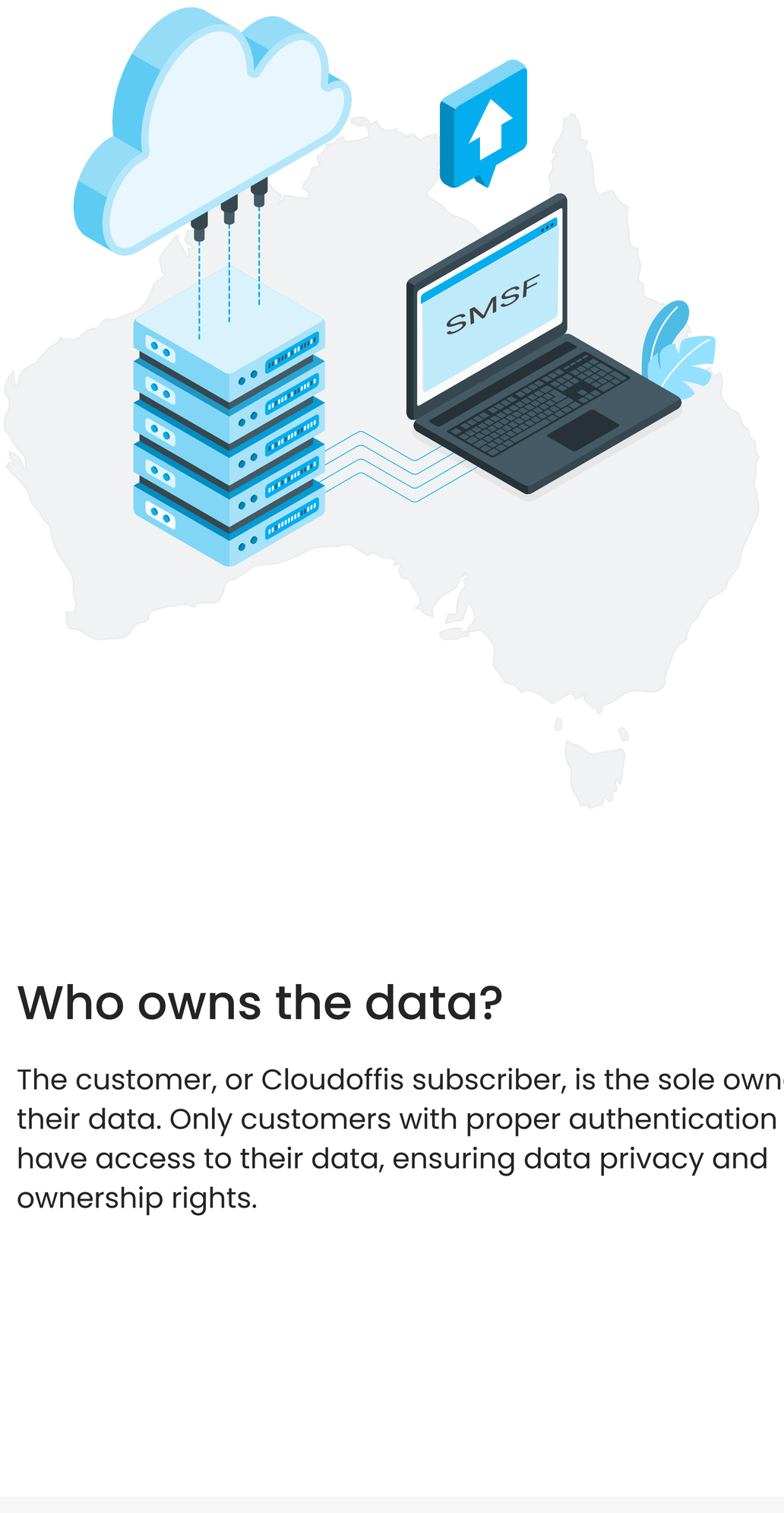
cloudoffis

Data Security

Our secure data practices enhance your customers' trust in you

At Cloudoffis, data security is our top priority throughout our operations. Our commitment to safeguarding the personal data of both you and your customers is reflected in every aspect of our system design and architecture.

Below, we outline our data storage, ownership, security measures and disaster recovery procedures, designed to keep you and your clients information safe, 24/7.

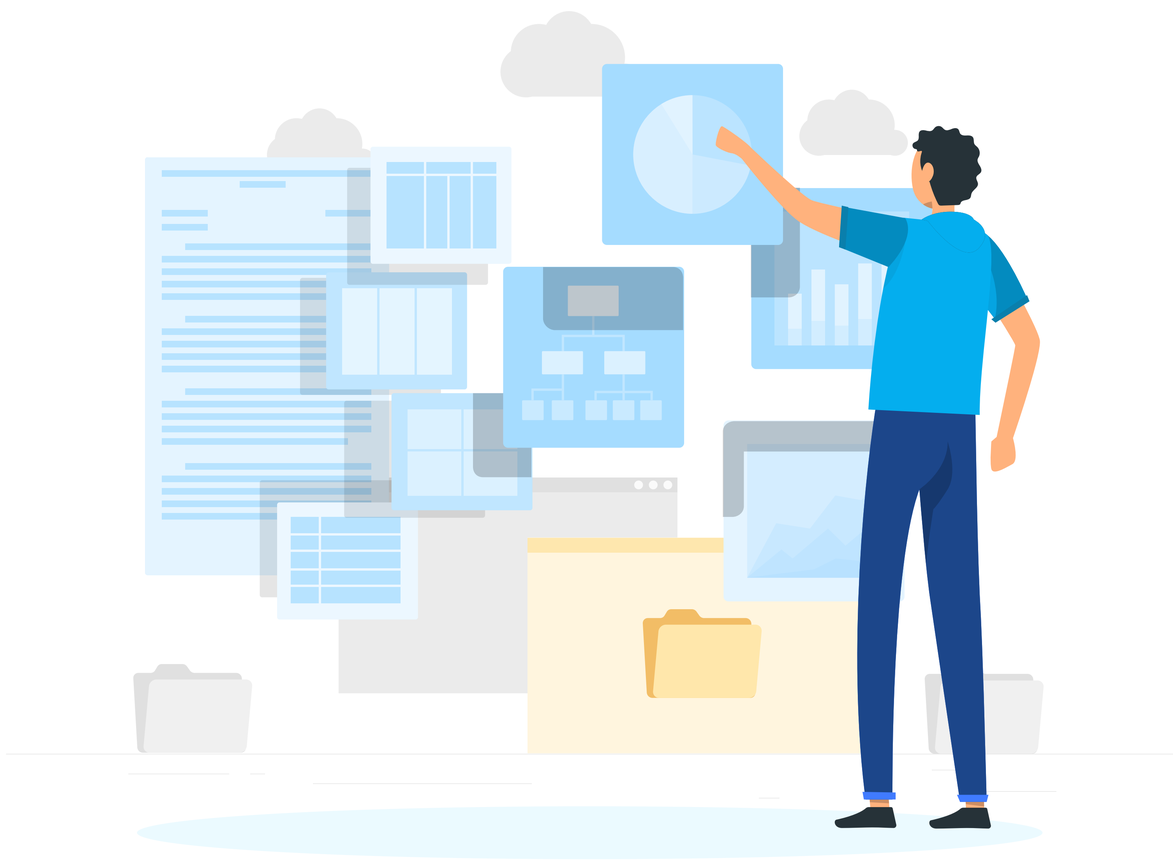


Where is the data stored?

All customer data, including production data, is stored in Australia. We utilise Amazon Web Services (AWS) servers in Australia, ensuring your data remains within the country. AWS is ISO 27001 compliant, adhering to international standards.

Who owns the data?

The customer, or Cloudoffis subscriber, is the sole owner of their data. Only customers with proper authentication have access to their data, ensuring data privacy and ownership rights.



How is data secured?

Below, we outline our data storage, ownership, security measures and disaster recovery procedures, designed to keep you and your clients information safe, 24/7.

Encryption

Data is encrypted both in transit and at rest, maintaining its confidentiality.

Distributed Storage

Data is stored in a distributed way, ensuring it's only accessible by authenticated users through the Cloudoffis platform.

Secure coding

Our product engineering team follows secure coding practices to prevent vulnerabilities, in line with the OWASP Top 10 guidelines.

Role-Based Access

Employees, managers, and administrators have role-based access levels, ensuring that users can only view data relevant to their responsibilities.

Infrastructure Security

Access to our infrastructure is highly restricted, with advanced security protocols and protective measures, including web application firewalls.

Penetration testing

Regular third-party penetration tests are conducted to identify and rectify any potential vulnerabilities

Segregated Environments

We maintain separate environments and databases for different stages of product development.

Proactive Maintenance

We proactively patch and update our infrastructure to safeguard against vulnerabilities.

Monitoring

Our IT infrastructure is monitored using enterprise-grade tools to detect issues early and take corrective action.

Multi-Factor Authentication

We offer MFA capabilities on every user account to enhance security.

Data Transmission Security

We encrypt data transmission with TLS 1.2 or improved versions, providing secure communication

Backup and Disaster Recovery

We ensure the availability and reliance of our systems through AWS's managed services

Data Backup

AWS's backup services provide dynamic offsite backups, disaster recovery, and multiple site synchronisation

Minimal Data Loss

In the event of a disaster recovery event, the maximum period of modified data that could be lost is 15 minutes

Rapid Recovery

Our disaster recovery plan ensures that data and services can be restored within a maximum of 1 hour

Regular Testing

Our disaster recovery procedures are rigorously tested on a quarterly basis to guarantee their effectiveness

Your Privacy

Review our privacy policy for more information.

If you have any further questions about the security of the data stored in Cloudoffis, please get in touch at support@cloudoffis.com.au and we will happily share more information.