Data and information security

empower®
by AdviserPlus

How can you be confident that your data is in safe hands?

One of our primary responsibilities at AdviserPlus is to ensure that there is a secure environment for all company and client information and to ensure business continuity. Our data processing complies with all applicable data protection laws and regulations.

AdviserPlus has established and maintains an information security management system which is considered best practice and complies with the requirements of the Information Security Management standard ISO27001:2017. Security objectives are set to demonstrate commitment to the continuous improvement of the system. Cyber security is taken seriously and AdviserPlus is certified to the Cyber Essential Plus scheme.

Below are some of the key considerations for your data security:

1 Where will our people data be stored?

All data is stored in the Microsoft Azure Cloud in the UK, we have geo-replication between South and West UK regions.

2 Will our data be encrypted?

Data entering AdviserPlus is typically encrypted using PGP, inbound data is sent encrypted in transit using TLS 1.2 to our Secure File Servers. We then segregate all stored data in client dedicated databases. Any files are persisted to Azure Storage and are encrypted at rest using AES256. All servers are patched up-to-date and have anti-virus, anti-malware and network threat protection software installed.

3 What protection does the database have?

All applications are accessed securely via TLS/SSL. We can offer additional layers of security such as IP Whitelisting. Internally all data access is audited and controlled using Role Based Access Control. Additionally we can offer traditional Forms Based Authentication or work with our clients to support Single Sign on via SAML2.0.

4 How do you test that our data is kept secure?

We conduct quarterly internal penetration tests and contract the services of external CREST-approved penetration testers to evaluate our systems annually. Executive summary and any remediation reports are shared with clients. We utilise a combination of Web Application Filtering (WAF), advanced threat monitoring and intrusion detection systems to maintain our security posture.

5 Who is responsible for keeping our data secure?

AdviserPlus' information security policies, associated processes and procedures must be adhered to by management, staff, contractors and temporary workers and they may impact visitors, suppliers and customers. AdviserPlus ensures that all relevant parties are fully conversant with its objectives through staff induction programme and on-going training and education programmes where necessary.

6 Do you have a disaster recovery plan in place?

Our disaster recovery plan centres around replication of our cloud services using ASR (Automatic Site Recovery). Our RTO timescale is four hours following the invocation of our disaster recovery plan.

Full technical information is available upon request

adviserplus.com
empowermymanagers@adviserplus.com
0844 327 2293

empower® by AdviserPlus