Data and Application Security

Last Modified on 01/07/2021 8:53 am BST

Data and Application Security

Synaptic Software adheres to the strictest standard of data and information security policies. The public version of these policies are available upon request.

Policies for Information Technology Security, Data Management Security, Personnel Security, Physical Security and Legal and Regulatory Compliance are in place. Policy compliance is adhered to through regular reporting and annual risk assessments.

All personnel are vetted when recruited and regular mandatory training programmes are in place for adhering to security policies.

We operate all our online services in state-of-the-art, secure data centers with the following features:

- Accredited to ISO9001, ISO20000 and ISO 27001 standards
- The data centre is subject to regular audits, assessments and inspections by certification bodies, regulators and accreditors
- The Synaptic databases are held electronically on secure dedicated servers only accessible by Synaptic named and authorised employees
- Services are mirrored between two data centre locations within the UK (over 50 miles apart) with near-instant failover capabilities

By outsourcing our server hosting in this way then in the case of any unforeseen event, Synaptic are able to replicate operations with little or no disruption to the services we provide to our customers. Access to all of our clients' data is restricted to Synaptic named and authorised individuals only.

Transport level security

- Secure two-way authentication (or bilateral authentication) where both client and server authenticate themselves to each other using public key certificates and encryption
- Any movement of data between physical data centres is completed through encrypted site to site VPN connections and all data is encrypted during transmission
- All data is transferred using transport layer security TLS 1.2 or higher

Application level security

- Application-level security is based on XML frameworks defining message confidentiality, integrity, authenticity and message structure
- A unique secure application level token is issued for the duration of a session
- All networks and systems used in development and operation of services sit behind EAL-4 standard firewalls
- Each server has IDS/IPS systems at the perimeter with a central management and alerting systems

- Each service has a separate DMZ, Application zone and Database zone, which are segregated by internal firewalls
- Our publicly accessible products are predicted by an additional Web Application Firewall service.

All development follows the OWASP best practice guidelines, which provides a framework for security and privacy by design. Synaptic acts as a data processor for its clients and therefore we have the strictest data protection controls in place to support the compliance requirements for data controllers.

We never share data with any third parties unless contracted and authorised to do so.

Data Processing

Categories of Data Subjects

Data subjects include client's representatives and end clients; such as client's employees, contractors and their customers.

Categories of Personal Data

The personal data processed concern the following categories of data:

Client personal data

•Personal data may include, among other information, personal contact information such as name, business address, business telephone or mobile number, fax number, email address, and passwords

Customers of the client

•Personal data derived from authorised users use of the services such as information concerning family, lifestyle and social circumstances including age, date of birth, employment details including job title and salary as well as name, email addresses and postal addresses

•Special category data: To process certain types of quotations some medical data is collected, such as smoker status

Controller of Data

The control of personal data remains with client. Client is responsible for compliance with its obligations as data controller under data protection legislation, in particular for justification of any transmission of personal data to the company (including providing any required notices and obtaining any required consents), and for its decisions concerning the processing and use of the data.

Purpose of processing

The personal data transferred will be subject to the following basic processing activities:

- Personal data will be processed to the extent necessary to provide the services in accordance with both the agreement and the controller's instructions. The processor processes personal data only on behalf of the controller. Processing operations include, but are not limited to:

- Acquisition and storage of client credential data so that the services can be used.
- Acquisition and storage of client's customer data so that quotations can be obtained through the service as well as providing financial product recommendations, product valuations and ongoing servicing of their financial needs
- Technical support, issue diagnosis and error correction to ensure the efficient and proper running of the systems and to identify, analyse and resolve technical issues both generally in the provision of the services and specifically in answer to a controller query. This operation may relate to all aspects of personal data processed but will be limited to metadata where possible.

The company will reserve the right to anonymise personal data for aggregation purposes where all personal data identifiers have been removed and re-identification made impossible.

Cross border and onward transfer of data

We will not store or directly transfer the personal data / special category data outside of the EEA.

However, an authorised user who uses the service to process personal data using a computer outside of the EEA may affect a transfer of data outside of the EEA.

Data retention period

We will retain personal data relating to the customer and the customer's customer if the authorised user is contracted with the company to use the service. When authorisation to use the system seizes, all data related to the customer and their customer's data will be deleted within 35 days.

All personal data relating to a specific quotation, including all messaging between the client and product providers, will be available for 95 days. Thereafter all personal data relating to the specific transaction will be permanently deleted from the system and be no longer accessible to the client nor the company.

Rights of Data Subject

Due to the transactional nature of the services provided and validity periods set by the provider, the data entered into the system is available for that specific transaction only.

The client has the right to withdraw their consent for their personal data being stored within the service ensuring contractual minimum term agreements are followed. Client is responsible for managing their client's consent and has been granted a process for deleting personal details relating to that data subject.

The company is not regulated by a supervisory authority as a software vendor. Client is responsible for data subject's complaints to the industry regulator the Financial Conduct Authority.

None of the services provided by Synaptic Software provide any automated decision making.