Data Processing and Information Security

January 2019

Contents

Purpose of this document 2
Company Details 3
Selectapension Overview 3
Data Processing 4
Types of Data Processed 5
Data Storage 5
Data Retention 5
Data Transfer 6
Security 6
Data Subject Access Requests 7
Audits and Inspections 7
Data Breaches 7
Appendix - Technical Architecture 8
Technical Specification 8
Architecture 8
Multi Device Support 8
Browsers 8
Accessibility 8
Security Model 9
Reliability 9
Minimum Infrastructure Requirements 9
Expected Performance 9
Scalability 9
Hosting Provider Rackspace IT Hosting 10

Purpose of this document

This document is intended as an overview of Selectapension Limited (Selectapension) preparedness for GDPR and explains how we process the personal data of your clients and the measures we've implemented to protect the data from security threats and data breaches. We hope it provides re-assurance that we take information security very seriously at Selectapension.

If you have any queries or suggestions they can be directed to:

Data Protection Officer: gdpr@selectapension.com

Company Details

Organisation Name	Selectapension Limited
Postal Address	Selectapension House, Eridge Road, Crowborough, East Sussex, TN6 2SL
Telephone	01892 669494
Web	www.selectapension.com
Registration Number	05075441
Data Protection Registration Number	Z8764990
Email	gdpr@selectapension.com
Data Role	Data Processor

Selectapension Overview

Founded in 2004, Selectapension Limited is the leading provider of online retirement and investment planning technology solutions to the UK retail financial services industry, with over £44 billion analysed each year. The Company is a private Limited Company and is therefore independent and unbiased.

Selectapension offers a comprehensive suite of online Pension and Investment planning modules, providing highly detailed analyses in a user-friendly package with client facing reports.

Our tools comprise Money Purchase, Provider Comparison, With Profits and Funds, Income Drawdown and Annuity Suite, Asset Reviewer, Retirement Planner and DB TVAS.

Selectapension is a Data Processor.

The services are provided on a subscription basis, with a minimum initial contract of 12 months. Customers access the tools through a secure login on the Selectapension Limited website. They input their client data onto the tools and download their completed analysis reports, in PDF format, via the website.

Data Processing

Any reference in this document to 'Client' means an individual who will be the recipient of financial advice.

Any references to 'Customer' means an individual or firm that pays for subscriptions to Selectapension Limited and who are therefore Data Controllers.

Purpose of processing	The personal data of clients supplied to Selectapension is used for the sole purpose of analysing and comparing financial products specified by the subscribing Financial Advice Firm.
Types of data processed	Minimal personal data of client – Name, DoB, Gender, Marital Status, General Health status (Good, Average, Poor)
Legal grounds for processing	1. Performance of a contract 2. Legitimate Interests

Subscribers provide personal data to Selectapension via its website. To become a subscriber and use the website, organisations must register and agree to Selectapension's terms and conditions of use.

Subscribers confirm, when they accept our Terms and Conditions of use, that they have the necessary consent of their clients to input their personal data onto the Selectapension system.

Authorised users are issued with unique login credentials to access the website. They can then input their clients' personal data onto the Selectapension system.

The user application is solely accessed via the web browser, data is input into the screens presented and the data is then passed back securely to the server for processing. User input is validated - there are a number of fields within the system that have automatic validation contained within them, i.e. numeric characters or alpha characters only can be entered.

Selectapension also offers a Report Writing Service whereby the customer sends Selectapension the input data, either by email or phone for comparison. Our employees then input the data onto the Selectapension system, create the report and email it back to the customer.

Types of Data Processed

The personal data required to complete an analysis is listed below:

Title, Name, Date of Birth, Gender, Marital Status, Basic Health Status, Spouse's DoB, Spouse's Gender.

Our data input templates are available here.

Processing Duration

The duration of processing depends on the user. Assuming that all the data and information required to complete an analysis is available, processing can be completed in half an hour.

Data Storage

Selectapension Ltd uses Rackspace in the UK to host our analysis application and database servers. Rackspace is ISO/IEC 27001 certified. Our data hosting supplier monitors and protects against Denial of Service (DOS) attacks. The servers are monitored 24/7 to protect against DOS attacks, and any unauthorised access. We also monitor usage of the system on a monthly basis and would be aware of any inappropriate usage levels.

https://www.rackspace.com/en-gb/compliance

The PDF reports generated by our tools are stored on AWS. AWS is certified with ISO/IEC 27001 for technology, ISO 27017 for cloud security, ISO 27018 for cloud privacy,

https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/

Reports are stored securely and indefinitely in order to comply with FCA COBS 9: Suitability (including basic advice)(non-MiFID) Clause 9.5.2 (1).

https://www.handbook.fca.org.uk/handbook/COBS/9.pdf

Data Retention

Selectapension Ltd retains the client reports created on its platform in order to comply with FCA requirements FCA COBS 9: Suitability (including basic advice)(non-MiFID) Clause 9.5.2 (1). **https://www.handbook.fca.org.uk/handbook/COBS/9.pdf**

Upon written request, Selectapension will either return to the data controller or securely wipe from its systems, any personal data in accordance with requirements of data protection legislation, where not prohibited by regulatory authorities.

Data Transfer

Selectapension has integrations with the following firms. Data may only be transferred between parties where a user has subscriptions and appropriate logins to both services.

Recipient Organisation	Purpose	Location	Transfer Mechanism
AssureWeb (iPipeline)	Annuity Quick Quote	UK	Token & Encrypted API
IRESS – X-Plan & Adviser Office	Back Office Integration	UK	Encrypted API
Fairstone	Back Office Integration	UK	Encrypted API
True Potential	Back Office Integration	UK	Encrypted API

Security

How do you secure any communications or browser sessions?	All communication between browsers and our application servers is via SSL, using VeriSign certificates. Cookies are also encrypted.
How do you secure any data held or collected?	An absolute minimum of personal data is held / collected (e.g. name, date of birth, gender, for both client and partner where appropriate). This is held in a dedicated database with Active Directory controlled access.
How do you ensure data is securely disposed of?	Data is not routinely disposed. In case of system failure or hardware replacement, our application host adopts WEEE guidelines for data disposal.
How do you control access to the systems?	Active Directory accounts provide restricted access to databases and file systems controlled by our own technical team.
How is physical access controlled to the servers?	Host data centres use 24 hour security personnel, CCTV, electronic and biometric codes and sign in procedures, zoned areas, and guests must provide photo id and be approved for entry.
How is client / user authentication handled and how is the data held?	Users access the system using a username and an application generated password which cannot be changed (following introduction of GDPR, users will generate their own password by a secure method). Passwords are stored using SHA-2 hashing algorithm. Selectapension will not have access to customers' passwords.
How do you control and maintain access rights to functionality within your application?	This is implemented at application level, and controlled via a custom internal-only administration interface that connects to a database linked to the user accounts.

Data Subject Access Requests

Any request for data should be requested in writing, from the client in question, and they should be fully identified before any information is released. Requests should be addressed to:

The Data Protection Officer
Selectapension Limited
Selectapension House
Eridge Road
Crowborough
East Sussex, TN6 2SL

enquiries@selectapension.com

- If a request is received directly from a client, Selectapension will inform their advice firm within 48 hours of receiving the request.
- Selectapension will provide a copy of the information free of charge. However, we may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.
- Selectapension may also charge a reasonable fee to comply with requests for further copies of the same information.
- The fee will be based on the administrative cost of providing the information.
- Information will be provided at the latest within one month of receipt of any verified Subject Data Access Request.
- Selectapension may extend this period by a further two months where requests are complex or numerous. If this is the case, Selectapension will inform the individual within one month of the receipt of the request and explain why the extension is necessary.
- If the request is made electronically, Selectapension will respond in the same format or any commonly used media.

Audits and Inspections

Selectapension shall provide reasonable assistance to our customers to ensure they are both meeting their GDPR Article 28 obligations, and will assist in submitting to reasonable audit and inspection requests.

Data Breaches

Selectapension has mechanisms in place to notify the customer without undue delay on becoming aware of any data breach, and any notifiable breach will be reported within 72 hours of Selectapension becoming aware.
Selectapension has not suffered any data breaches.

Appendix - Technical Architecture

Technical Specification

The Selectapension platform is an enterprise-class architecture built on the industry standard Microsoft .NET framework. Going forward there will be a continual programme of following and supporting the latest proven versions of the Microsoft technology stack.

The Selectapension platform has been designed as a logically and physically tiered solution, utilising service orientation to expose function, systems and data to an appropriately authenticated and authorised audience.

Third party applications may interact with the platform via the Selectapension API. This is exposed as a clearly documented set of SOAP based web services, providing necessary lookup lists and calculation functions in order to allow a third party to emulate the input process employed within Selectapension's own web site calculators, process calculations, and receive results sets suitable for rendering within their own environment.

Architecture

The Selectapension platform is built on a multi-tier architecture of: a) User Interface (UI), b) Services and c) Data. A key design characteristic of the platform is that it can be split both vertically and horizontally.

Horizontally, the application splits presentation, application and data. This allows the application to be flexible when meeting client's requirements, whether these are deployment, scaling, performance or customisation. For example, a custom presentation capability can be implemented that calls the business services exposed by the application tier, or maybe forgone completely if the client is only interested in exposing services to an orchestration layer.

Vertically, the platform implements a set of business specific functional areas that can be delivered in isolation to each other. Consequently, the client organisation can just implement those functional areas (or even specific subsets of those functional areas) which meet its business requirements.

A full System Architecture Design document that supports the Selectapension platform can be made available upon request.

Multi Device Support

The platform provides native support for PCs, tablets and smartphones (all major browsers) from a single code base delivering device plug-and-play as standard.

Browsers

Conformance with XHTML doctype standards while using CSS 2.1/3.0 allows us to support most modern browsers. This includes browsers such as Firefox (and other Mozilla incarnations), Safari, IE8+, Edge and Chrome. Going forward, the application will support the two latest versions of a supported browser. Where possible XHTML5.0 will be used, where the functionality is supported across the target platforms.

Accessibility

To meet the UK Disability Discrimination Act (DDA) requirements the presentation tier supports WCAG 2.0 AA with one exception. The single exception is the use of java script. The presentation tier will

cater for graceful degradation if java script functionality is not present, but the advantages of java script far outweigh excluding it from the standards.

Security Model

Both the application and all customer data is fully secured from external and internal attack by using the latest tools and techniques, this minimises reputational risk and maximises control and commercial confidence.

Reliability

Reliability is a key architectural behaviour within the platform; this is supported through a resilient design where a deployment can be configured without a single point of failure. A recommended deployment would involve the provision of a web farm of multiple stateless and identically configured servers within the presentation and application tiers, offering both resilience and scalability. This is complemented with supporting instrumentation to enable operational monitoring staff to easily review the health of the infrastructure in real-time and take pro-active or remedial action as required.

Minimum Infrastructure Requirements

The Selectapension platform supports hosting on a Microsoft Windows Operating System platform, namely Windows Server 2003 or later, however Windows Server 2008 is recommended for new implementations. The database server can be based upon Microsoft SQL Server 2005 SP3 or later, again SQL Server 2008 is recommended. Additional pre-requisites include the availability of the Microsoft Internet Information Server (IIS) Windows Component for hosting web applications and services and a pre-installation of the Microsoft .NET frameworks.

As the Selectapension platform architecture is logically and physically tiered, deployment options for the solution are versatile and support variants ranging from a single server deployment to the provision of three tier environment containing:

- A web farm of identically configured presentation servers
- A web farm of identically configured application servers
- A distributed cache cluster
- A SQL Server instance with failover provisioning (dependent upon business continuity and disaster recovery requirements)

Expected Performance

The Selectapension platform is based upon a proven and highly scalable architecture that has been designed to support both horizontal and vertical scaling in order to meet the capacity and throughput requirements of our expected customer structures. Whilst every implementation is different, our standard expectation is that the system will typically provide sub-second page response times at the server for the majority of screen pages.

Scalability

Scalability is another key architectural behaviour of the platform and as an enterprise class solution it can be configured to process the business volumes required by a wide range of organisations from small IFA firms to enterprise level organisations through the use of horizontal and / or vertical scaling of the infrastructure. Selectapension work with clients to determine the transactional quantities and use our performance modelling approach to ensure the optimal infrastructure configuration to meet the anticipated business needs.

Hosting Provider Rackspace IT Hosting

FACILITIES DESCRIPTION

LON3 Data Centre – Slough, UK

FACILITY

- Data Centre floor space is approximately 5,000 square meters of raised floor.
- Site is manned 24x7x365 with Rackspace Operations personnel.
- OEM service/maintenance contracts on all facility infrastructure systems.
- SSAE16 compliant.

SECURITY

- Physical access to devices within Rackspace data centres is restricted to authorized Rackspace personnel.
- Card reader and biometric access required to enter facility.
- Card reader access required to enter data centre floor.
- Security cameras recorded by digital video recorder.
- Bomb proof film installed behind all windowed areas.
- Fully fenced perimeter.

POWER

- 100% renewable energy.
- Facility rated at 1.75kW per square meter or 3.5kW per rack.
- Two separate 15 MVA utility feeds provide power to the DC.

UPS

- Four 1,200 kW Chloride UPS Net90 Clusters (N+1 configuration), expandable to 1,600 kW per Cluster.
- Two 1,000 kW Chloride UPS Trinergy Clusters (modular N+1 configuration), expandable to 1,600 kW per Cluster.
- 78 UPS power distribution panels.
- UPS-fed panels are fully redundant.
- UPS provides instantaneous conditioned power for facilities until generator synchronization; transfer of power is automatic.
- 10 minutes battery life at peak load.

GENERATOR

- Six 2.25 MVA AVK diesel generators (N+1 configuration), expandable to eight.
- Generators activate and fully synchronize within 60 seconds.
- Each generator has its own supply system with a total of 60,000 litres on site.
- Fuel suppliers under contract to deliver fuel within 4 hours.
- 36-hour on site fuel capacity under full load.

HVAC

- 1,461,843 m^3/h of cooling capacity.
- One Hundred and Four CRACs computer room air handling units (N+25% configuration).
- Seven 1,500 kW RC Group centrifugal chillers w/VSD (N+1 configuration), expandable to eight.
- Six chilled water loop pumps, and condenser water loop pumps (N+1 configuration).

FIRE PROTECTION

- Early Smoke Detection (VESDA).
- Dry pipe pre-action fire suppression system.

FACILITY MONITORING

- NARC – Network monitoring software.
- Trend Facility Monitoring System (BMS).
- C-Matic Power Management System allows real time monitoring and trending of power utilisation.

CUSTOMER ACCESS

- Customers retain administrative control of their leased servers.
- Rackspace retains control of dedicated networking hardware such as firewalls and load balancers.
- Console level access is provided via Terminal Services of SSH over VPN, depending upon platform.

BACKUP AND RECOVERY

- Fully managed backup to centralized storage is available; offsite tape rotation is optional.

NETWORK INFRASTRUCTURE

- Redundant Cisco 3-tier LAN Architecture.

PHYSICAL CONNECTIVITY

- Multiple fibre carriers.
- Copper and fibre installed and terminated to onsite demarcation.

TRANSIT

- Multiple Tier-1 Service Providers.
- 10-Gigabit Ethernet per carrier (multiple gigabits of total bandwidth available).

ROUTING

- Redundant Cisco 6500 Series and ASR 9000 Series Switches for edge and core routing.
- Internap FCP route optimization.

SWITCHING

- Cisco 3550/3750/4948 Series Switches for aggregation.
- Cisco 2950/2960/2970 Series Switches for distribution.