Data Processing Agreement (DPA)

This Data Processing Agreement including its Attachments ("***DPA***") is between Selectapension Ltd. ("***Supplier***") and the entity that receives any Products from Supplier ("***Customer***") pursuant to a written or electronic agreement which governs the provision of those Products ("***Agreement***"), and shall apply to the extent that (i) Supplier Processes Personal Data on behalf of the Customer, and (ii) either the Agreement expressly incorporates this DPA by reference or the parties sign this DPA.

This DPA is supplemental to, and forms an integral part of, the Agreement and is effective upon the earlier of signature or its incorporation into the Agreement ("**Effective Date**"), which incorporation may be specified in the Agreement or an executed amendment to the Agreement. In case of any conflict or inconsistency between the terms of the Agreement and this DPA, this DPA shall take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

The term of this DPA shall follow the Term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

1. Definitions

"*Controller*" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"*Data Privacy Laws*" means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Privacy Laws; in each case to the extent applicable and as amended, repealed, consolidated or replaced from time to time.

"*Data Subject*" means the individual to whom Personal Data relates.

"***DORA***" means Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

"*European Personal Data*" means Personal Data that is subject to European Privacy Laws.

"*European Privacy Laws*" means data protection and privacy laws applicable in the European Union, the European Economic Area ("**EEA**") and/or their member states, Switzerland and the United Kingdom, in each case as hereinafter amended, superseded, or replaced, including:

i. Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("***GDPR***");

ii. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC;

iii. Applicable national implementations of (i) and (ii); the Data Protection Act of 2018; and GDPR as it forms part of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (collectively "***UK GDPR***"); and

iv. Swiss Federal Act on Data Protection of 19 June 1992 (as amended 25 September 2020) and its Ordinance ("***FADP***").

"*Instructions*" means the written, documented instructions issued by Customer to Supplier and directing the same to perform a specific or general action with regard to Personal Data.

"*Onward Transfer*" means a transfer of Personal Data from a third-party, such as a Processor, to a fourth-party, such as a Sub-Processor, or beyond.

"*Permitted Affiliates*" means any of Customer's Affiliates (as defined under the Agreement):

(i) That are permitted to use the Products pursuant to the Agreement, but have not signed their own separate agreement with Supplier;

(ii) For whom Supplier Processes Personal Data; and

(iii) That are subject to Data Privacy Laws.

"*Personal Data*" means any information provided by or collected on behalf of Customer relating to an identified or identifiable individual where such information is protected under applicable Data Privacy Laws as personal data, personal information, personally identifiable information, or any equivalent thereof.

"*Personal Data Breach*" means an event that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Supplier and/or its Sub-Processors in connection with the provision of the Products, subject to any limitations, exclusions, exceptions, or safe harbors provided for by applicable Data Privacy Laws. "Personal Data Breach" shall not include (a) any such events for which notification is not required pursuant to applicable Data Privacy Laws, or (b) unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems, except to the extent that any such unsuccessful attempts or activities must be disclosed pursuant to applicable Data Privacy Laws.

"*Processing*" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms "Process", "Processes" and "Processed" will be construed accordingly.

"*Processor*" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

"Products" means the goods and services provided by Supplier to Customer under the Agreement.

"*Standard Contractual Clauses*" or "**SCCs**" means, for the processing of Personal Data that is subject to the GDPR, the standard contractual clauses approved pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021, as available at http://data.europa.eu/eli/dec_impl/2021/914/oj, as they may be amended, superseded, or replaced. For the Processing of Personal Data that is subject to the UK GDPR, the Standard Contractual Clauses also include the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/, as it may be amended, superseded, or replaced (the "**UK Addendum**").

"*Sub-Processor*" means any third-party engaged by Supplier to carry out specific Processing activities in accordance with the Instructions and subject to further limitations set forth in this DPA.

"*Third Country*" means, for the Processing of Personal Data that is subject to the GDPR, UK GDPR, or FADP, a country that is not a member of the EEA, United Kingdom, or Switzerland, respectively, and not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Privacy Laws).

2. Roles of the Parties

To the extent that European Privacy Laws apply to the Processing activities under the Agreement, the parties acknowledge and agree that Supplier is a Processor and Customer is either (i) a Controller, or (ii) a Processor acting on behalf of a Controller that is not a party to the Agreement or this DPA.

3. Customer Responsibilities

a. **Compliance with Laws.** Customer shall be responsible for complying with all its obligations under applicable Data Privacy Laws and shall inform Supplier without undue delay if it is not able to comply with its responsibilities under this sub-section (a) or applicable Data Privacy Laws. In particular but without prejudice to the generality of the foregoing, Customer acknowledges and agrees that it shall be solely responsible for:

i. the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data;

ii. complying with all necessary transparency and lawfulness requirements under applicable Data Privacy Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorisations (particularly for use by Customer for marketing purposes);

iii. ensuring it has the right to transfer, or provide access to, the Personal Data to Supplier for Processing in accordance with the terms of the Agreement (including this DPA);

iv. ensuring that its Instructions to Supplier regarding the Processing of Personal Data comply with applicable laws, including Data Privacy Laws; and

v. complying with all laws (including Data Privacy Laws) applicable to any content created, sent or managed through the Products, including those relating to obtaining consents (where required) to send communications, the content of the communications, and its communication deployment practices.

b. **Instructions.** The parties agree that the following constitutes Customer's complete and final Instructions to Supplier in relation to the Processing of Personal Data: (i) the terms of the Agreement and this DPA, including the Attachments hereto, (ii) direction from Customer through its use of the Products in accordance with the Agreement, and (iii) this general authorisation by Customer which hereby permits Supplier to use Personal Data for any business operations incident to providing the Products to Customer. Additional instructions outside the scope of the Instructions must be agreed to according to the process for amending the Agreement or this DPA, where applicable.

c. **Security**. Customer is responsible for independently determining whether the data security provided for in the Products adequately meets its obligations under applicable Data Privacy Laws. Customer is also responsible for its secure use of the Products, including protecting account access to the Products and the security of Personal Data in transit to and from the Products (including the secure backup or encryption of any such Personal Data).

4. Supplier Obligations

a. **Compliance with Instructions.** Supplier shall only Process Personal Data for the purposes described in this DPA, including Attachment 1, or as otherwise agreed within the scope of Customer's lawful Instructions, except where and to the extent otherwise permitted by applicable law. Supplier is not responsible for compliance with any Data Privacy Laws applicable to Customer or Customer's industry that are not generally applicable to Supplier.

b. **Conflict of Laws.** If Supplier becomes aware that it can no longer meet its obligations under the applicable Data Privacy Laws or Process Personal Data in accordance with Customer's Instructions due to a legal requirement under any applicable law, Supplier will:

i. promptly notify Customer of that legal requirement to the extent permitted by the applicable law; and

ii. where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as Customer issues new Instructions with which Supplier is able to comply. If this provision is invoked, Supplier will not be liable to Customer under

the Agreement for any failure to provide the applicable Products until such time as Customer issues new lawful Instructions with regard to the Processing.

c. **Technical and Organisational Measures.** Supplier shall implement and maintain appropriate technical and organisational measures to protect Personal Data from Personal Data Breaches, as described under Attachment 2 (*Technical and Organisational Measures*) to this DPA. Notwithstanding any provision to the contrary, Supplier may modify or update the contents of Attachment 2 at its discretion provided that such modification or update does not result in a material degradation in the technical and organisational measures set forth therein.

d. **Confidentiality.** Supplier shall ensure that any personnel whom Supplier authorises to Process Personal Data on its behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

e. **Personal Data Breaches.** In the event that Supplier becomes aware of any Personal Data Breach, Supplier will notify Customer without undue delay, and in any case within any time period set forth in applicable Data Privacy Laws. Customer hereby agrees that Supplier may, in its discretion, provide any legally required notices of Personal Data Breaches to applicable authorities and/or affected Data Subjects, provided that Customer shall have the right to propose commercially reasonable edits to any such notices; otherwise, if Supplier defers to Customer to provide any such notices then Supplier shall provide Customer with such reasonable assistance as necessary to enable Customer to provide any such notices. Customer may, at its own effort and expense, send any notices that are not required by applicable law.

f. **Deletion or Return of Personal Data.** Supplier will Process Personal Data for the duration of the Agreement only, unless otherwise agreed in writing. Supplier will delete or return all Personal Data (including copies thereof) Processed pursuant to this DPA on termination or expiration of the Products in accordance with the procedures and timeframes set out in the Agreement. Notwithstanding the foregoing and subject to applicable Data Privacy Laws, Supplier may continue to retain Customer's Personal Data for as long as necessary to comply with Supplier's legal and regulatory obligations; to enable fraud monitoring, detection and loss prevention activities; to comply with Supplier's tax, accounting, and financial reporting obligations; and where required by Supplier's contractual commitments to third-parties. Any such processing that extends beyond the term of the Agreement shall be done in accordance with the terms of this DPA and any applicable Data Privacy Laws.

g. **Demonstration of Compliance**. Supplier shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and applicable Data Privacy Laws and shall allow for and contribute to audits, including inspections by Customer, in order to assess compliance with this DPA and applicable Data Privacy Laws. Customer acknowledges and agrees that it shall exercise its audit and inspection rights under this DPA by instructing Supplier to supply, on a confidential basis, (i) copies of its current Cyber Essentials and Cyber Essentials Plus certificates and an executive summary of its most recent independent penetration test, along with copies of any related policies and other documentation, or its hosting provider's security programs and related policies and documentation if Supplier does not host the Personal Data itself, or (ii) written responses to all reasonable requests for information made by Customer necessary to confirm Supplier's compliance with this DPA, along with copies of any related policies and other documentation. Customer shall not exercise this right to audit and inspect more than once per calendar year.

h. **Supplier Assistance to Customer**. To the extent required by applicable Data Privacy Laws, Supplier shall assist Customer with Customer's obligations under those applicable Data Privacy Laws. Such assistance may be provided through Product functionality, in which case Customer agrees to utilize such functionality before asking Supplier for further assistance.

5. Data Subject Requests

As part of Supplier's obligation under Section 4(f) above, where required by applicable Data Privacy Laws, Supplier will assist Customer with Customer's obligation to respond to requests from data protection authorities and Data Subjects that seek to exercise their rights under applicable Data Privacy Laws ("***Data Subject Requests***"). All Data Subject Requests must provide sufficient information for Supplier to verify the identity of the Data Subject. Customer shall reimburse Supplier for any commercially reasonable costs that arise from any such assistance that is in addition to that which Supplier normally provides to its customers.

If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to Supplier, Supplier will, to the extent that Supplier can identify Customer as the source of the Personal Data in question through its standard due diligence processes, promptly inform Customer of such Data Subject Request and will advise the Data Subject to submit their request to Customer. Customer shall otherwise be solely responsible for responding to any Data Subject Requests.

6. Data Protection Assessments

To the extent required by applicable law, Supplier will provide reasonable assistance to Customer to enable Customer to conduct and document data protection assessments, provided that the required information is reasonably available to Supplier, and Customer does not otherwise have access to the required information.

7. Sub-Processors

Customer agrees that Supplier may engage Sub-Processors to Process Personal Data on Customer's behalf. Customer hereby approves, as Sub-Processors, the entities on the list of Sub-Processors located below. Any desired changes to the list of Sub-Processors must follow the amendment process set forth in Section 11(a) of this DPA.

Where Supplier engages Sub-Processors, Supplier will execute a written agreement with any Sub-Processor that imposes data protection and privacy terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors. Supplier will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause Supplier to breach any of its obligations under this DPA.

The list of approved Sub-Processors is as follows:

Entity	Country of Origin	Purpose
Microsoft	United Kingdom	Cloud hosting, compute, storage and backup for the application (Microsoft Azure, UK South with replication to UK West); email and collaboration (Microsoft 365)
Perseus Management Group Inc.	United States of America	Administration and support of the Microsoft 365 environment (email and other office productivity tools)
CrowdStrike	United Kingdom	Managed endpoint detection and response; processes endpoint security telemetry
Proofpoint	United Kingdom	Inbound email filtering and attachment scanning; processes email content in transit

8. Location of Supplier Processing

Customer acknowledges that Supplier will Process Personal Data in the United Kingdom as necessary to provide the Products in accordance with the Agreement. Supplier shall ensure that any such Processing which

requires a transfer of Personal Data outside of Customer's country will be done in accordance with the requirements of applicable Data Privacy Laws.

9. Additional Provisions for European Personal Data and DORA

a. **Scope.** This Section 9 (*Additional Provisions for European Personal Data*) shall apply only with respect to European Personal Data. In the event that the terms and conditions in this Section 9 conflict with those in the other sections of this DPA, the terms and conditions in this Section 9 shall take precedence.

b. **Data Protection Impact Assessments and Consultation with Supervisory Authorities.** To the extent required by European Privacy Laws, Supplier will provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities, provided that the required information is reasonably available to Supplier, and Customer does not otherwise have access to the required information.

c. **Transfer Mechanisms for Cross Border Transfers.**

i. Supplier shall not transfer, or permit any of its Sub-Processors to transfer, European Personal Data to any Third Country, unless it first takes all such measures as are necessary to ensure the transfer will be made in compliance with applicable European Privacy Laws. Such measures may include (without limitation) transferring such data to a recipient that has (A) a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, (B) achieved binding corporate rules authorisation in accordance with European Privacy Laws, or (C) executed appropriate standard contractual clauses as adopted or approved in accordance with applicable European Privacy Laws and conducted any requisite data transfer impact assessments in conjunction therewith.

ii. The Standard Contractual Clauses will apply if, and only to the extent that, Personal Data is transferred, either directly or via Onward Transfer, to any Third Country, (each a "***Cross Border Transfer***").

A. With respect to Cross Border Transfers from the EEA or Switzerland to a Third Country, the iteration of the Standard Contractual Clauses set forth in Part 1 (EEA/Swiss Transfers) of Attachment 3 shall apply.

B. With respect to Cross Border Transfers from the United Kingdom to a Third Country, the iteration of the Standard Contractual Clauses set forth in Part 2 (UK Transfers) of Attachment 3 shall apply.

iii. Notwithstanding Section 9(c)(ii), the Standard Contractual Clauses will not apply to a Cross Border Transfer if Supplier has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Cross Border Transfers.

iv. If and to the extent the Standard Contractual Clauses (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict.

d. **DORA**. To the extent that DORA applies to the Processing activities under the Agreement, the parties acknowledge and agree that the terms of Attachment 4 and Attachment 5 shall apply.

10. General Provisions

a. **Amendments.** Notwithstanding anything else to the contrary in the Agreement and without prejudice to Section 4(a) (*Compliance with Instructions*), or Section 4(c) (*Technical and Organisational Measures*), Supplier reserves the right to make any updates and changes to this DPA or list of Sub-Processors. Any such modifications become effective thirty (30) days after the date that Supplier either (1) notifies Customer that the updated DPA or list of Sub-Processors has been posted to a particular URL, or (2) distributes the updated DPA or list of Sub-Processors to any known point-of-contact for Customer. Customer is responsible for reviewing and becoming familiar with the updated DPA or list of Sub-

Processors. If, prior to the effective date of the updated DPA or list of Sub-Processors, Customer notifies Supplier of its objection to any modification of the DPA or list of Sub-Processors, then Supplier shall either (i) negotiate with Customer in good faith to resolve any such objection, or (ii) upon thirty (30) days' notice to Customer, terminate the DPA and any portion of the Agreement that governs Products which are dependent upon its execution. If Supplier exercises its right to terminate pursuant to the terms of this Section, Customer shall be entitled to a pro-rata refund of any Fees already paid by Customer for the affected Products, calculated from the effective date of any such termination.

b. **Severability.** If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

c. **Limitation of Liability.** Each party's liability, and where applicable, each of Customer's Affiliates' liability, taken in aggregate, arising out of or related to this DPA, including the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, shall be subject to the limitations and exclusions of liability set out in the Agreement. In no event shall either party's liability be limited with respect to any individual Data Subject's data protection and privacy rights under this DPA(including the Standard Contractual Clauses) or otherwise.

d. **Governing Law.** This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Privacy Laws.

11. Parties to this DPA

a. **Permitted Affiliates.** Customer enters into this DPA (including, where applicable, the Standard Contractual Clauses) on behalf of itself and, to the extent required under applicable Data Privacy Laws, in the name and on behalf of its Permitted Affiliates, thereby establishing a separate DPA between Supplier and each such Permitted Affiliate. Each Permitted Affiliate agrees to be bound by the obligations under this DPA. For each separate DPA that is established, the Permitted Affiliate shall be the "Customer."

b. **Authorisation.** The legal entity entering into this DPA as Customer represents that it is authorised to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

c. **Remedies.** Except where applicable Data Privacy Laws require a Permitted Affiliate to exercise a right or seek any remedy under this DPA against Supplier directly by itself, the parties agree that: (i) solely the Customer entity that is the contracting party to the Agreement shall exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all communication with Supplier under the DPA and shall be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.

Selectapension Ltd Registered Office: Pine Grove Enterprise Centre, Pine Grove, Crowborough, East Sussex, TN6 1DH
Registered in England & Wales: 05075441

Attachment 1 – Details of Processing

A. Nature and Purpose of Processing

Supplier will Process Personal Data for the limited and specific purposes identified in the Agreement, including as necessary to provide the Products pursuant to the Agreement, as further specified in an Order Form or SOW, and as further instructed by Customer in its use of the Products. Personal Data may also be used for the following Processing activities: (a) use as necessary to maintain the Products provided to Customer; (b) use of Personal Data of Customer's personnel to provide Support Services and account management (invoicing, customer success, etc.); and/or (c) disclosure to third-parties in accordance with the Agreement, this DPA, or as compelled by applicable laws, which may include sending Personal Data to Customer's partners and service providers on Customer's behalf and at their direction.

B. Duration of Processing

Subject to Section 4(f) (*Deletion or Return of Personal Data*) of this DPA, Supplier will Process Personal Data for the duration of the Agreement only, unless otherwise agreed in writing.

C. Categories of Data Subjects

Customer may provide Personal Data relating to the following categories of Data Subjects to Supplier in the course of using the Products, or incident to the use thereof, the extent of which is determined and controlled by Customer in its sole discretion:

Customer's employees, contractors, collaborators, customers and their dependants and spouses/partners, business partners, prospects, suppliers and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to Customer's end users.

D. Categories of Personal Data

Customer may provide the following categories of Personal Data to Supplier in the course of using the Products, or incident to the use thereof, the extent of which is determined and controlled by Customer in its sole discretion:

- Contact Information, including name, mailing address, email address, online user name(s), telephone number, and similar information, country of residency
- Financial information, including payment account information and salary
- Pension information
- Gender
- Professional or employment related information, including place of employment and job title
- Marital status
- National Insurance number
- Date of Birth
- Any other Personal Data submitted by, sent to, or received by Customer, or Customer's end users, via the Products

E. Special categories of data (if appropriate)

The parties may process the following special categories of Personal Data or sensitive personal information, as those terms are defined under applicable Data Privacy Laws:

- Health Data

Selectapension Ltd Registered Office: Pine Grove Enterprise Centre, Pine Grove, Crowborough, East Sussex, TN6 1DH
Registered in England & Wales: 05075441

Attachment 2 – Technical and Organisational Measures

Supplier shall comply with its obligations as a Processor under the Data Privacy Laws to keep all Personal Data secure. Without limiting the foregoing, Supplier shall: (a) taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to applicable Data Privacy Laws; and (b) in assessing the appropriate level of security, taking into account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. Such measures include (as applicable), without limitation:

a) Access Control

Outsourced Processing: Supplier Processes Customer's Personal Data, including Personal Data that is used in conjunction with its hosted Software and Cloud Services, using industry-leading, reputable cloud infrastructure vendors. Supplier maintains contractual relationships with these infrastructure vendors which obligates them to provide their infrastructure services in accordance with standards which conform to the requirements of applicable Data Privacy Laws and that are no less restrictive than this Data Processing Agreement.

Physical and environmental security: Supplier hosts its Cloud Services in multi-tenant environments and deploys industry best practices with respect to isolating each tenant from one another. Customer Data is held in a shared database, with access controlled through role based authorisation so that users may access only data belonging to their own organisation. Customers access data only through the application user interface and application programming interfaces, and have no direct access to the underlying database or infrastructure.

Authentication: Supplier has implemented strong password policies for all systems that Process Customer's Personal Data. Customers who interact with the Products via the user interface must authenticate before accessing non-public Personal Data.

Authorisation: For Cloud Services, Personal Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces, and Customers are not allowed direct access to the underlying application infrastructure. For all systems that Process Customer's Personal Data, the authorisation model in each of Supplier's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customisation options. Authorisation to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorisation.

Access controls: Supplier implements industry standard access controls for all systems that Process Customer's Personal Data. Network access control mechanisms are designed to prevent network traffic using unauthorised protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: Supplier implements industry standard intruder detection capabilities for all systems that Process Customer's Personal Data. Supplier has implemented a Web Application Firewall (WAF) solution to protect all internet-accessible systems that Process Customer's Personal Data. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in Supplier's source code repositories are regularly performed, checking for logical errors, security flaws, and performance flaws.

Vulnerability testing: Supplier conducts regular vulnerability testing of systems that Process Customer's Personal Data. These vulnerability tests are intended to identify and resolve foreseeable attack vectors and potential abuse scenarios.

Product access: A subset of Supplier's employees have access to the Products and other systems that Process Customer's Personal Data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents, and implement data security measures. Access is enabled through "just in time" requests for access, and all such requests are logged. Employees are granted access by role, and reviews of high-risk privilege grants and roles are conducted regularly.

External access to Supplier systems that Process Customer's Personal Data is restricted, following the same least privilege model, and requires two-factor authorisation and authentication. External access controls are configured and monitored by Supplier IT and Security personnel.

Background checks: All Supplier employees who access systems that Process Customer's Personal Data undergo a background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

Access control to premises and facilities: In addition to the access control measures stated above in this subsection (a), the following measures apply to Supplier's office premises:

Supplier operates no on-premise server infrastructure. All Customer Data is hosted in Microsoft Azure data centres within the United Kingdom, where physical access is controlled by Microsoft under their certified controls. At Supplier's office premises, physical access is controlled by electronic fob at entry and exit points, with all access logged. CCTV covers all building entry and exit points, with footage retained for 30 days. The premises are secured by alarm. Visitors are logged and subject to identity checks on arrival. Sensitive equipment is protected against power failure. Physical security controls are verified annually as part of Cyber Essentials Plus assessment. As part of annual Security Awareness Training, Supplier staff are trained in concepts of physical security and understand procedures for contacting security personnel if needed.

b) Transmission Control

In-transit: For Supplier Products that are accessible via the Internet, Supplier makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces. Supplier's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Supplier stores user passwords following policies that follow industry standard practices for security. Supplier has implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: Supplier designed its infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Supplier personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Supplier maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, legal, operations, or support personnel, and appropriate resolution steps are identified and documented. For any confirmed incidents, Supplier will take appropriate steps to respond and notify Customer in accordance with the terms of this DPA.

Selectapension Ltd Registered Office: Pine Grove Enterprise Centre, Pine Grove, Crowborough, East Sussex, TN6 1DH
Registered in England & Wales: 05075441

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99% uptime. The infrastructure providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer's Personal Data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods. Supplier's systems that Process Customer's Personal Data are designed to ensure redundancy and seamless failover. The server instances that support the Products are also architected with a goal to prevent single points of failure. This design assists Supplier operations in maintaining and updating the Product applications and backend while limiting downtime.

Measures to ensure that personal data are protected from accidental destruction or loss: Supplier has business continuity, incident response, data backup, and disaster recovery procedures designed to maintain business operations and redundancy of systems that Process Customer's Personal Data. Supplier performs regular testing to ensure that availability supporting systems function properly.

e) Certifications

Upon request of Customer, Supplier will provide copies of its current Cyber Essentials and Cyber Essentials Plus certificates, an executive summary of its most recent independent penetration test, and written responses to reasonable requests for information, along with copies of related policies and documentation. Supplier does not hold a SOC 2 report or ISO 27001 certification.

Selectapension Ltd Registered Office: Pine Grove Enterprise Centre, Pine Grove, Crowborough, East Sussex, TN6 1DH
Registered in England & Wales: 05075441

Attachment 3

Part 1 – EEA/Swiss Transfers

1) The parties agree that the terms of the Standard Contractual Clauses, as supplemented by this Part 1, are hereby incorporated by reference and shall apply to the transfer of Personal Data from the EEA or Switzerland to Third Countries.

2) Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the transfer of Personal Data to a Third Country is effectuated by Customer as the Controller of the Personal Data and Supplier is the Processor of the Personal Data.

3) Module Three (Processor to Processor) of the Standard Contractual Clauses shall apply where the transfer of Personal Data to a Third Country is effectuated by Customer as the Processor of the Personal Data and Supplier is a Sub-Processor of the Personal Data.

4) The parties acknowledge that the Standard Contractual Clauses solicit input from the parties in several clauses, and the parties agree that the following responses shall apply (to Module Two and Module Three, where applicable):

   a) Clause 7 of the SCCs shall not be applicable.

   b) In Clause 9(a), Option 2 (general written authorisation) shall apply, the time period for prior notice of Sub-Processor changes shall be thirty (30) days.

   c) In Clause 11, the optional language will not apply, and Data Subjects shall not be able to lodge a complaint with an independent dispute resolution body.

   d) In Clause 17, option 1 shall apply. The Parties agree that the Standard Contractual Clauses shall be governed by the laws of the Republic of Ireland.

   e) In Clause 18(b), the parties choose the courts of the Republic of Ireland as their choice of forum and jurisdiction.

5) Annex I.A of the SCCs shall be completed as follows (for Module Two and Module Three):

   a) **“Data Exporter”:**

      i) **Name:** The entity identified as “Customer” in the DPA

      ii) **Address:** The address for Customer associated with its account or as otherwise specified in the DPA or Agreement.

      iii) **Contact person’s name, position and contact details:** The contact details associated with Customer’s account, or as otherwise specified in the DPA or the Agreement.

      iv) **Activities relevant to the data transferred under these Clauses:** The activities specified in Attachment 1 of the DPA.

      v) **Role (controller/processor):** With respect to Module Two, Controller; with respect to Module Three, Processor.

   b) **“Data Importer”:**

      i) **Name:** Selectapension Ltd.

      ii) **Address:** Pine Grove Enterprise Centre, Pine Grove, Crowborough, East Sussex TN6 1DH

      iii) **Contact person’s name, position and contact details:** Adrian Malin, Managing Director, Adrian.malin@selectapension.com

      iv) **Activities relevant to the data transferred under these Clauses:** The activities specified in Attachment 1 of the DPA.

v) **Role (controller/processor):** With respect to Module Two, Processor; with respect to Module Three, Processor.

c) Signature and Date: By entering into the DPA, data exporter and data importer are deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the DPA.

6) Annex I.B of the SCCs shall be completed as follows (for Module Two and Module Three):

a) **Categories of data subjects whose personal data is transferred:** Categories of data subjects are specified in Attachment 1 of the DPA.

b) **Categories of personal data transferred:** The personal data is described in Attachment 1 of the DPA.

c) **Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:** The data exporter will transfer the sensitive Personal Data listed in Section E of Attachment 1 to the DPA (if any). To the extent that data importer receives sensitive Personal Data, data importer will apply those restrictions or safeguards that are necessary and appropriate based on applicable Data Privacy Laws.

d) **The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):** Personal data is transferred on a continuous basis.

e) **Nature of the processing:** The nature of the processing is described in Attachment 1 of the DPA.

f) **Purpose(s) of the data transfer and further processing:** The purpose of the processing is described in Attachment 1 of the DPA.

g) **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:** Personal Data will be retained for the later of (i) the date upon which data exporter asks data importer to delete or destroy the Personal Data in accordance with the terms of the DPA or the Agreement, and (ii) as long as permitted by applicable Data Privacy Laws.

h) **For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing:** The subject matter, nature and duration of the processing are described in Attachment 1 of the DPA.

7) **Annex I.C** of the SCCs shall be completed as follows: The competent supervisory authority in accordance with Clause 13 of the Standard Contractual Clauses is the supervisory authority in the Member State stipulated in Section 4(d) of this Attachment 3.

8) Attachment 2 to this DPA (Technical and Organisational Measures) serves as **Annex II** of the SCCs.

9) Section 7 of this DPA (Sub-Processors) serves as **Annex III** of the SCCs.

Part 2 – UK Transfers

1) The parties agree that the terms of the Standard Contractual Clauses, as supplemented by Part 1 above and amended by the iteration of the UK Addendum attached hereto as Exhibit 1 to Attachment 3 of this DPA, are hereby incorporated by reference and shall apply to the transfer of Personal Data from the United Kingdom to Third Countries. The Standard Contractual Clauses, together with the UK Addendum, which are deemed to be amended to the extent necessary to enable them to: (a) lawfully facilitate transfers by the data exporter to the data importer, to the extent that UK Data Privacy Laws apply to such transfers; and (b) provide appropriate safeguards for the transfer in accordance with Articles 46 of the UK GDPR.

2) This Part 2 shall (a) be read and interpreted in the light of the provisions of UK GDPR and so that it fulfils the intention for it to provide the appropriate safeguards as required by Article 46 of the UK GDPR, and (b) not be interpreted in a way that conflicts with rights and obligations provided for in the UK GDPR.

3) Any references to legislation, including the UK Addendum, mean that legislation, as may be amended from time to time (including consolidation, reenactment or replacement of such legislation following the Effective Date of this DPA).

4) To the extent there is any conflict between the Standard Contractual Clauses, together with the UK Addendum, and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses, together with the UK Addendum, will prevail.

Exhibit 1 to Attachment 3 – International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

Part 1: Tables

Table 1: Parties

Start date	Upon the effective date of the DPA.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: As stated in Part I, Section 5(a) of Attachment 3 to the DPA Trading name (if different): _____ Main address (if a company registered address): As stated in Part I, Section 5(a) of Attachment 3 to the DPA Official registration number (if any) (company number or similar identifier): _____	Full legal name: As stated in Part I, Section 5(b) of Attachment 3 to the DPA Trading name (if different): _____ Main address (if a company registered address): As stated in Part I, Section 5(b) of Attachment 3 to the DPA Official registration number (if any) (company number or similar identifier): _____
Key Contact	As stated in Part I, Section 5(a) of Attachment 3 to the DPA	As stated in Part I, Section 5(b) of Attachment 3 to the DPA
Signature (if required for the purposes of Section 2)	NOT REQUIRED	NOT REQUIRED

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: June 4, 2021 template, effective on the Start Date listed above Reference (if any): _____ Other identifier (if any): _____ Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Selectapension Ltd Registered Office: Pine Grove Enterprise Centre, Pine Grove, Crowborough, East Sussex, TN6 1DH
Registered in England & Wales: 05075441

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As stated in Part I, Section 5 of Attachment 3 to the DPA
Annex 1B: Description of Transfer: As stated in Part I, Section 6 of Attachment 3 to the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As stated in Part I, Section 8 of Attachment 3 to the DPA
Annex III: List of Sub processors (Modules 2 and 3 only): As stated in Part I, Section 9 of Attachment 3 to the DPA

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Selectapension Ltd Registered Office: Pine Grove Enterprise Centre, Pine Grove, Crowborough, East Sussex, TN6 1DH
Registered in England & Wales: 05075441

Attachment 4

1. Roles of the Parties – DORA

To the extent that DORA applies to the Processing activities under the Agreement, the parties acknowledge and agree that Supplier is an ICT third-party service provider and Customer is a financial entity, as those terms are defined under DORA.

2. Personal Data

Personal Data, as that term is defined in Section 1 of this DPA, shall also include all data that is governed by DORA.

3. DORA Termination Rights

In addition to any termination rights granted to Customer under the Agreement, Customer may terminate the Agreement on 30 days' written notice if:

a. Supplier is in significant breach of DORA and related regulations or terms of this DPA;

b. Circumstances arise that are capable of altering Supplier's provision of the Products under the Agreement such that Supplier is no longer and can no longer continue to provide the Products in a manner that is in material compliance with Customer's or Supplier's obligations under DORA;

c. There are documented material deficiencies in the way Supplier ensures the availability, authenticity, integrity and, confidentiality, of data that is governed by DORA such that Supplier cannot provide the Products in a manner that is in material compliance with Customer's or Supplier's obligations under DORA; and

d. The competent authority, as applicable pursuant to Article 46 of DORA, can no longer effectively supervise the Customer as a result of the conditions of, or circumstances related to, the Agreement.

4. ICT Security

Supplier will participate in the Customer's ICT security awareness programmes and digital operational resilience training upon request and at Customer's expense.

5. SLAs

Supplier shall ensure to Customer continuation of the guaranteed level of availability of the Products. Service levels are set out in Attachment 5 to the DPA.

Attachment 5

1. Data Backup and Disaster Recovery

a. Backups.

i. Supplier shall maintain backups of the Cloud Services, including all Customer Data that is created or stored within the Cloud Services. Database backups shall be taken no less frequently than every fifteen (15) minutes, with a full backup taken weekly, providing point-in-time restore capability. Backups shall be encrypted and immutable, and shall be replicated to a geographically separate Microsoft Azure region within the United Kingdom, at least ten (10) miles from the site where the Cloud Services are hosted. Backup retention shall be no less than thirty (30) days.

ii. Supplier shall maintain backups as follows:

Compute		Storage		Disaster Protection (Facility)	
Backup	**Retention**	**Backup**	**Retention**	**Source**	**Recovery**
Every 15 mins (database); weekly full	30 days	Every 15 mins (database); weekly full	30 days	Backup	4 hr. RTO 15 min. RPO

b. Disaster Recovery.

i. Supplier shall maintain a "**Disaster Recovery Plan**" which includes plans to restore access to the Cloud Services in response to an event, whether natural or caused by human action, that results in an unintended loss of data or access to the Cloud Services ("**Disaster Event**"). Disaster Events can arise from (A) natural disasters, such as earthquakes or floods, (B) technical failures, such as power failure or network connectivity, and (C) human actions, such as inadvertent misconfiguration or unauthorised/outside party access or modification

ii. Supplier shall conduct annual disaster recovery testing as a part of its Disaster Recovery Plan.

iii. If either Party discovers a Force Majure event that would trigger a Disaster Recovery Plan, it shall promptly notify the other Party by email with the applicable details.

c. "**Recovery Point Objective**" or "**RPO**": the point in time prior to a Disaster Event to which Customer Data shall be recoverable shall be no longer than fifteen (15) minutes.

d. "**Recovery Time Objective**" or "**RTO**": in response to a Disaster Event, Supplier shall restore Customer's access to the Cloud Services within four (4) hours of what can reasonably be determined to be the end of the Disaster Event.

2. Downtime and Technical Support Incident Response

a. For the duration of the Term, the Cloud Services shall be available to Customer during Business Hours, except for unavailability that may result from a "**Permissible Downtime Event**," as defined below. "Business Hours" means 09:00 to 17:00 United Kingdom time on any day other than a Saturday, Sunday or English public holiday.

i. Permissible Downtime Events include:

A. Force Majeure event(s), as defined in Section 15 of the GTCs;

B. Acts or omissions of the Customer or its employees, agents, contractors, or representatives;

C. The Customer's failure to follow and/or implementation instructions or procedures issued by Supplier;

D. Use or failure of any Customer owned or provided hardware, software, or other components used in connection with the Cloud Services;

E. Failure of the Customer's internet provider, telecommunications circuit, or internet backbone outages, routing, or peering issues that prevents communication between Customer and Supplier's data centre(s);

F. Emergency maintenance resulting from critical and time sensitive security exploits and threats, or other maintenance with the intent to protect the confidentiality, integrity, and availability of Customer's and/or Supplier's systems and data, and/or safety or care of either parties' employees and/or associates; and

G. Downtimes resulting from critical security threats and exploits originating from Customer and/or Customer's login credentials.

ii. Permissible Downtime Events do not include any length of time in excess of the RTO in response to a Disaster Event. Permissible Downtime Events notwithstanding, the total aggregate availability of the Cloud Services during Business Hours in any one calendar month shall not be less than 99% ("**Uptime Warranty**"). Availability outside Business Hours is not measured and does not count towards the Uptime Warranty.

3. Support Incident Process

a. Generally. When you contact Supplier for Support Services:

i. Every service request (incident) is logged into the support system as a traceable ticket and is accessible to all members of the technical support team;

ii. The technical support team assigns the incident a priority based, in part on the Severity Level (as defined hereinbelow) indicated by Customer; and

iii. If after reasonable troubleshooting, unresolved incidents are escalated to Supplier's engineering team for resolution.

b. Severity Level Definitions. The Severity Level definitions are as follows:

Severity Level	Definition
Severity 1 (Sev-1)	**Critical Service Outage** A production service is down, and no workaround is immediately available. • A critical production service – such as workstation access, signature signoff, web server, configuration server, database server, or other server - is down or not responding and cannot be stabilized or restarted. • Customer's business operations have been severely disrupted. • >50% of users on a platform or server are affected. • May not be used in the case of a new installation, a test server or platform, or where no production users are on the system. Severity 1 support requires you to have dedicated resources available to work on the issue on an ongoing basis. In the case that the Customer cannot continue to work on the issue with Supplier, the case Severity Level may be reduced to a Sev-2. A service outage does not include the loss of connectivity or access for a single or relatively small subset of users, and a service outage should only be filed on issues thought to be problems with the server or service.
Severity 2 (Sev-2)	**Major Functionality** Major functionality is severely impaired. • Operations can continue in a restricted fashion, although productivity might be

Selectapension Ltd Registered Office: Pine Grove Enterprise Centre, Pine Grove, Crowborough, East Sussex, TN6 1DH
Registered in England & Wales: 05075441

Severity Level	Definition
	adversely affected. • A major milestone is at risk. Ongoing and incremental installations are affected. • A temporary workaround is available.
Severity 3 (Sev-3)	**Minor Functionality** Minor functionality not working; a workaround is available. Partial, non- critical loss of functionality of the software. • Impaired operations of some components but allows the user to continue using the software. • Initial installation milestones are at minimal risk.
Severity 4 (Sev-4)	**General Usage Questions** • Cosmetic issues, including errors in the documentation. • General configuration or use questions. • Upgrade, major change, and migration notifications. • Enhancement requests. • Incidents initially opened via email are assigned a Severity Level of Sev-3.

c. Target Response Times. Each Severity Level has a corresponding Target Response Time listed in the table below. For the sake of clarity, the Target Response Time is not a reference to the time it will take for an incident to be resolved. The Target Response Times are measured from the time an issue has been submitted by Customer in accordance with this Attachment. Target Response Times apply during Business Hours only. An issue submitted outside Business Hours is treated as submitted at the start of the next Business Hours period.

Severity Level	Target Response Time
Critical Service Outage (Sev-1)	30 Minutes (Business Hours)
Major Functionality (Sev-2)	1 business hour
Minor Functionality (Sev-3)	4 business hours
General Usage Questions (Sev-4)	16 business hours

Selectapension Ltd Registered Office: Pine Grove Enterprise Centre, Pine Grove, Crowborough, East Sussex, TN6 1DH
Registered in England & Wales: 05075441