DATA PROCESSING ADDENDUM

Where applicable, this Data Processing Addendum is hereby incorporated in the SoftStart Terms of Service (the "**Terms**"), found at https://softstart.app/terms-of-services/, unless Customer has entered into a superseding written agreement with Supplier, in which case, it forms a part of such written agreement. All capitalized terms not defined herein shall have the meaning set forth in the Terms. Unless Customer has a superseding written agreement with Supplier, Supplier may amend this Data Processing Addendum from time to time on its Website, as its business evolves. Any revisions will become effective on the date Supplier publishes the changes. Customer can review the most current version of the Data Processing Addendum at any time by visiting this page. If Customer uses the Services after the effective date of any changes, that use will constitute the acceptance of the revised Data Processing Addendum.

1. DEFINITIONS AND INTERPRETATION

(i) **"Customer Personal Information"** means any Personal Information contained within the information submitted or transferred by Customer or the Users to Supplier in conjunction with the usage of the SoftStart Platform (as defined in the Terms);

(ii) "**Data Controller**" has the meaning set out in the Privacy Laws, as applicable to this Data Processing Addendum;

(iii) "**Data Processor**" has the meaning set out in the Privacy Laws, as applicable to this Data Processing Addendum;

(iv) "**Data Protection Regulator**" means the applicable supervisory authority with jurisdiction over either party, and in each case any successor body from time to time;

(v) "**Data Subject**" has the meaning set out in the Privacy Laws, as applicable to this Data Processing Addendum;

(vi) "**Privacy Laws**" means all applicable data protection and privacy legislation, regulations and guidance governing the protection of Personal Information including but not limited to Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**") and the *Data Protection Act 2018* and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's *European Union (Withdrawal) Act 2018* (the "**UK GDPR**"), the California *Consumer Protection Act of 2018* (the "**CCPA**") and the California *Privacy Rights Act* (the "**CPRA**");

(vii) "**Process**", "**Processing**" or "**Processed**" have the meaning set out in the Privacy Laws, as applicable to this Data Processing Addendum.

(viii) **"2021 Standard Contractual Clauses"** means Standard Contractual Clauses for the transfer of Personal Information to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 or any European Commission's decision amending or replacing this decision.

(ix) **"Standard Contractual Clauses"** means collectively the 2021 Standard Contractual Clauses or the UK International Data Transfer Addendum whichever is applicable.

(x) **"UK International Data Transfer Addendum"** means the International Transfer Data Addendum to the 2021 Standard Contractual Clauses issued by the UK's Information Commissioner's Office.

2. PROTECTION OF PERSONAL INFORMATION

2.1. **Supersedence**. This Data Processing Addendum shall supersede any and all provisions of the Terms inconsistent herewith.

2.2. **Data Controller and Data Processor**. The Parties acknowledge that the Customer is the Data Controller and Supplier is the Data Processor of the Customer Personal Information. Supplier will Process Personal Information in accordance with Section 3 of this Data Processing Addendum.

2.3. **Customer's Obligations as Data Controller**. The Customer warrants that the Customer Personal Information has been obtained fairly and lawfully and, in all respects in compliance with the Privacy Laws.

2.4. **Supplier's Obligations as Data Processor**. Supplier shall:

2.4.1. Process the Customer Personal Information only in accordance with Section 3 of this Data Processing Addendum and any other reasonable documented instructions as provided by the Customer to Supplier from time to time ("**Instructions**"), including with regard to transfers of Customer Personal Information to a third country, save where:

2.4.1.1. such Instructions are unlawful;

2.4.1.2. such Instructions would cause Supplier to breach its own obligations under Privacy Laws or the Terms or any other agreement with a third party;

2.4.1.3. Supplier is under a legal obligation to Process the Customer Personal Information, in which case Supplier shall inform the Customer of the legal obligation, except to the extent the law prohibits it from doing so; and/or

2.4.1.4. such Instruction delays or prevents performance of the Services.

2.4.2. inform the Customer if, in its opinion, an Instruction received from the Customer infringes the Privacy Laws;

2.4.3. ensure that all Supplier employees and personnel who are involved in the Processing of Customer Personal Information have committed themselves to confidentiality or are under statutory obligations of confidentiality;

2.4.4. not provide any new third party, with access to the Customer Personal Information or sub-contract any of its obligations under the Terms that involve Processing Customer Personal Information without providing at least thirty (30) days advance notice to the Customer via email. The Customer hereby approves those third parties listed in Schedule 1 hereto (the "**Sub-processors**"), which are compliant with requirements under Privacy Laws, as applicable to this Data Processing Addendum, regarding transfers of Customer Personal Information to a third country.

2.4.5. ensure that any sub-contract entered into by Supplier (where Customer Personal Information is Processed by a Sub-processor) contains provisions which comply with Privacy Laws and in any event are no less onerous than those imposed under Section 2 of this Data Processing Addendum, and where a Sub-processor fails to fulfil its data protection obligations under the

Privacy Laws, Supplier shall remain liable to Customer for the performance of that Sub-processor's obligations;

2.4.6. implement and maintain appropriate technical and organizational security measures to protect against unauthorised or unlawful Processing of the Customer Personal Information and against accidental loss, disclosure or destruction of, or damage to, the Customer Personal Information, taking into account the state of the art, costs of implementation and nature, scope, context and purposes of Processing, as described in the Privacy Policy, found at https://softstart.app/privacy-policy/, and including:

2.4.6.1. the anonymization, pseudonymization and/or encryption of Customer Personal Information;

2.4.6.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

2.4.6.3. the ability to restore the availability and access to Customer Personal Information in a timely manner in the event of a physical or technical incident; and

2.4.6.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

2.4.7. taking into account the nature of the Processing, assist the Customer by appropriate technical and organizational measures, as further described in Schedule 2 hereto, to enable the Customer to comply with its obligations under Privacy Laws in responding to requests from Data Subjects or the Data Protection Regulator, insofar as this is possible;

2.4.8. assist the Customer (at the Customer's reasonable cost), to comply with the following obligations under the Privacy Laws, taking into account the nature of Processing and information available to Supplier, including:

2.4.8.1. notification and assistance to Customer without undue delay, in accordance with the provision set forth in Section 11 of the Privacy Policy, and notification to the Data Protection Regulator and Data Subjects of a breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Information transmitted, stored or otherwise Processed; and

2.4.8.2. the Customer's obligations to carry out data protection impact assessments and any subsequent consultation with the Data Protection Regulator;

2.4.9. make available to Customer or an independent third party auditor mandated by the Customer (but not being a competitor of Supplier) to a maximum of once a year or when a breach of Customer Personal Information is reasonably suspected, all reasonable information that Supplier deems necessary to demonstrate compliance with the obligations imposed on Supplier under Section 2 of this Data Processing Addendum, and allow for and contribute to audits, including inspections for the sole purpose of demonstrating such compliance;

2.4.10. unless required by law, at Customer's request following termination or expiry of the Terms for whatever reason, securely delete all of the Customer Personal Information;

2.4.11. comply with the relevant Controller to Processor provisions of the 2021 Standard Contractual Clauses which are incorporated by reference and are an integral part of this Data Processing Addendum, for the purpose of which the Parties agree that:

2.4.11.1. Customer is the data exporter and Supplier is the data importer.

2.4.11.2. Module Two of the 2021 Standard Contractual Clauses will apply where Customer is a Controller and Supplier is a Processor.

2.4.11.3. Clause 7 of the 2021 Standard Contractual Clauses will apply.

2.4.11.4. For the purpose of Clause 9, paragraph (a) of the 2021 Standard Contractual Clauses, option 2 shall apply, as per the time period specified under section **Erreur! Source du renvoi introuvable.** hereof.

2.4.11.5. The Parties agree that any direct claims brought under the Standard Contractual Clauses by a Party shall be subject to the limitation of liability set out in the Terms, provided however that nothing in this Data Processing Addendum shall be construed as a limitation or exclusion of a Party's liability toward a Data Subject under the Standard Contractual Clauses.

2.4.11.6. For the purpose of Clause 17 of the 2021 Standard Contractual Clauses the parties choose option 1 and the law of the Republic of Ireland.

2.4.11.7. For the purpose of Clause 18 of the 2021 Standard Contractual Clauses, paragraph (b), the Parties choose the courts of the Republic of Ireland.

2.4.11.8. The contents of Appendix I of the Standard Contractual Clauses are deemed completed with the information found in Sections 2 and **Erreur! Source du renvoi introuvable.** hereof. The contents of Appendix II are described in Schedule 2 hereof.

2.4.11.9. In the event of any conflict between the provisions of the Standard Contractual Clauses and this Data Processing Addendum, the Standard Contractual Clauses shall prevail.

2.4.12. comply with the UK International Transfer Addendum, as set out in Schedule 3 hereto.

2.4.13. **Additional Provisions for California**. To the extent that Supplier processes Personal Information of consumers subject to the CCPA, the CPRA and applicable regulations thereunder, the Parties shall comply with all applicable provisions of the CCPA, of the CPRA and of applicable regulations thereunder, as amended from time to time. The Parties shall agree to act in good faith to enter into a modified agreement in order to address any such amendment and ensure ongoing compliance with California laws. Supplier shall not (a) retain, use or disclose such Personal Information for any purpose

other than for the specific purposes described under the Terms or this Data Processing Addendum, or as otherwise permitted by the CCPA, the CPRA or applicable regulations; (b) retain, use or disclose such Personal Information for a commercial purpose other than the specific purposes described under the Terms or this Data Processing Addendum; or (c) “sell” or “share” such Personal Information (the terms “sell” and “share” having the meaning ascribed to them in the CCPA, CPRA or applicable regulations).

3. **INSTRUCTIONS FOR PROCESSING OF CUSTOMER PERSONAL INFORMATION**

Supplier will Process Customer Personal Information in accordance with the following instructions:

Categories of Customer Personal Information collected by Supplier	**Categories of Data Subjects for which Customer Personal Information is Processed**	**Purposes for which Supplier Processes Customer Personal Information**	**Nature of Processing**	**Duration of Processing**
Users credentials (such as emails, names, etc.) ➢ User credentials permit the Users to access the Supplier Platform and include emails and password hashes.	• account administrator that purchases the subscription and manages the account • account administrators, plan owners, coaches and collaborators which use the Platform to improve onboarding processes • employees and recruits using the Platform, answering the surveys and providing comments	• provide, maintain and improve the Supplier Platform • prevent or address service, security, support or technical issues with the Supplier Platform	• handling, storing, sharing with Sub-processors, accessing and reviewing Customer Personal Information for the Processing purposes set out adjacent	As long as necessary for the purposes described in this Data Processing Addendum, unless a longer retention is required by law.
Employee profiles ➢ The account administrator creates a profile for each of his/her employees, which contains the first name, last name, job title and email of the employee. Each employee has access to his/her employee profile and can update his/her information. The employee can also upload his/her own picture in his/her profile.	• account administrators, plan owners, coaches and collaborators which use the Platform to improve onboarding processes • employees and recruits using the Platform, answering the surveys and providing comments	• provide, maintain and improve the Supplier Platform • prevent or address service, security, support or technical issues with the Supplier Platform	• handling, storing, sharing with Sub-processors, accessing and reviewing Customer Personal Information for the Processing purposes set out adjacent	As long as necessary for the purposes described in this Data Processing Addendum, unless a longer retention is required by law.

[Signature page follows]

_____, referred to as "Customer" hereunder

Name: _____

Title: _____

Signature: _____ Date: _____

Laboratoire d’innovation technologique GSoft Inc.

Name: _____

Title: _____

Signature: _____ Date: _____

SCHEDULE 1: SOFTSTART SUB-PROCESSORS

Sub-processor	Microsoft, Inc.
Type of processing	Cloud Provider
Country	United States of America
Transfer Mechanism	Standard Contractual Clauses

Sub-processor	MongoDB, Inc.
Type of processing	Database management service
Country	United States of America
Transfer Mechanism	Standard Contractual Clauses

Sub-processor	trycourier.com, Inc.
Type of processing	Notification delivery service
Country	United States of America
Transfer Mechanism	Standard Contractual Clauses

Sub-processor	Merge API, Inc.
Type of processing	Unified API tool for provisioning multiple Human Resources Information Software (where HRIS integration is activated by Customer).
Country	Canada (data storage and processing) United States of America (access for support services)
Transfer Mechanism	Standard Contractual Clauses

SCHEDULE 2: GENERAL DESCRIPTION OF THE TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES IN PLACE

All capitalized terms not defined herein shall have the meaning set forth in the Terms.

Supplier has implemented and maintains the following technical and organizational security measures:

Pseudonymisation and encryption of Customer Personal Information	
Pseudonymisation	It is Supplier's policy to pseudonymize Customer Personal Information whenever possible. Supplier cannot pseudonymize the "User profile" data in the database, otherwise the managers could not view, add or modify data related to their employees.
Encryption	The data is encrypted in transit with HTTP over TLS. Certificates are 2048 bits and private keys are stored in a specific secret vault. The data is also encrypted at rest by Supplier and the Sub-processors. Encryption keys are managed with limited number of employees and secured in a vault with regular rotations.
Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services	
Confidentiality	Supplier has measures in place to ensure that no person is allowed to access Customer Personal Information without authorization. Such measures include, without limitation: • Supplier manages accesses to Customer Personal Information based on the role-based access control (RBAC) permissions model on a need to access basis and least privileged basis. • Supplier has a secure authentication process in place. • All Supplier employees are subject to a criminal background check to ensure that they are not guilty of a job-related offense. • Supplier's internal database is located at a MongoDB Atlas data center. MongoDB Inc. conforms to global security standards such as ISO 27001, PCI DSS, GDPR and SOC 2. • Supplier has measures in place to control physical security at its office (including security guard at building entrance, alarm system, visitor registration). • Supplier, all Supplier employees and Sub-processors have signed a non-disclosure agreement. • The data is encrypted in transit with HTTP over SSL. Certificates are 2048 bits and private keys are stored in a specific secret vault. Weak cyphers are disabled. The data is also encrypted at rest. Encryption keys are managed with limited number of employees and secured in a vault with regular rotations.

	• Regular updates concerning current security attacks are sent to Supplier's employees to raise awareness.

Integrity	Supplier has measures in place to ensure that the data integrity is maintained. Such measures include, without limitation:
	• The right to modify or delete any customer data (which includes Customer Personal Information) is restricted to a limited group of people on a need basis.
	  ○ Employees in the customer success team and in the technical support team are granted the right to modify and delete customer data in Supplier's database. Any modification or deletion by such employees is catalogued in an audit log. Supplier reviews accesses every two months and every time a team changes.
	  ○ Supplier restricts possible modifications and deletions within Supplier's database using role and permission-based access control rules.
	• Supplier maintains backups of its database in accordance with its internal retention rules.

Availability	Supplier has measures in place to ensure that Customer Personal Information is available and is used properly in the intended Process. Such measures include, without limitation: • Supplier maintains backups of its database in accordance with its internal retention rules. The backups are verified daily, and tests are done every three months to meet its RPO and RTO. • Supplier's infrastructure and is built from scripts that are kept in its source control system. Therefore, Supplier can deploy the whole infrastructure dynamically within hours. • Supplier has implemented Azure security center to prevent malware in the hosting environment and a centralized antimalware solution to prevent malware in the office with periodic full scans and firewall integration.
Resilience	Supplier has measures in place to ensure that the SoftStart Platform is resilient. Such measures include: • Supplier's infrastructure can scale automatically depending on the load. • Supplier's infrastructure is redundant in the same data center. • Supplier's database server is redundant in the same data center.
Ability to restore the availability and access to Customer Personal Information in a timely manner in the event of a physical or technical incident	
If causes of outage are within Supplier's control, its recovery time objective (RTO) is about 24 hours or less. The recovery point objective (RPO) is 12 hours. See measures described above with respect to "availability".	

Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing

- Access control: Supplier reviews accesses regularly and every time a team changes.
- Vulnerability assessments: Supplier performs regular internal penetration testing exercises.
- Logs centralization: Supplier has monitoring tools to collect, aggregate and analyze its logs.

Process for ensuring that access by government or law enforcement agencies is legally valid and appropriate

Supplier has procedures in place to ensure that Customer Personal Information cannot be accessed by governmental organizations or law enforcement without due process. Supplier and its Sub-processors will not disclose data to government or law enforcement agencies except as directed by Customer or where required by law. Supplier and its Sub-processors scrutinize all requests to validate that they are legally valid and appropriate. Upon receipt of such a request, Supplier will notify you, unless prohibited by law to do so. We will direct the governmental organization or law enforcement agency to seek the data directly from Customer by default. Where Supplier or its Sub-processors are legally bound to disclose information, only information specifically requested may be disclosed.

Our Sub-processors have committed to publish transparency reports regarding government and law enforcement requests for personal information. We do note however that only one of our Sub-processors (Microsoft Inc.) has been the object of such requests in recent years.

We note that the processed data is not the target of data gathering under Section 702 FISA or EO 12.333. There is no indication that such data has ever been the target of searches under Section 702 FISA or EO 12.333. Also, Section 702 FISA is only about communications services provided to the targets of the searches, and not to others or applications such as the present one. Therefore, we believe that the probability that Supplier or its Sub-processors will receive a surveillance order with respect to Customer Personal Information is very low.

SCHEDULE 3: UK INTERNATIONAL DATA TRANSFER ADDENDUM

Purpose. This Schedule supplements the Data Processing Addendum as incorporated by reference to the Terms to govern the international transfer of Personal Information out of the United Kingdom. By signing the Terms, the Parties agree to the terms of this Schedule.

PART 1: TABLES

Table 1 will be completed with the Parties' details as set out in the Terms.

TABLE 2 - Selected SCCs	
Addendum EU SCCs	The 2021 Standard Contractual Clauses, including the appendix information as set out in Section 2.4.11 of the Data Processing Addendum.

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 2021 Standard Contractual Clauses (other than the Parties), and which for this Addendum is set out in:	
Annex 1A	List of Parties: As described in Section **Erreur! Source du renvoi introuvable.** of the Data Processing Addendum.
Annex 1B	Description of Transfer: As described in Section **Erreur! Source du renvoi introuvable.** of the Data Processing Addendum.
Annex II	Technical and organisational measures including technical and organisational measures to ensure the security of the data: As described in Schedule 2 to the Data Processing Addendum.
Annex III	List of Sub Processors: As described in Schedule 1 to the Data Processing Addendum.

TABLE 4 - Ending this Addendum	
Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum: Exporter and Importer

PART 2: MANDATORY CLAUSES

Mandatory Clauses incorporated by this express reference: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf	Incorporation by reference of Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and submitted to Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 and approved on 21 March 2022, as amended from time under Section 18 of those Mandatory Clauses.