Saaswedo USA Inc, located 1175 Peachtree St. NE in Atlanta, GA 30361, USA and represented by Christian Cor
(hereinafter, « the processor »)

of the one part,

AND

[ ], located [ ],
in [ ], [ ] represented by [ ]
(hereinafter, « **the controller** »)

of the other part,

I. Purpose

The purpose of these clauses is to define the conditions in which the processor undertakes to carry out, on the controller's behalf, the personal data processing operations defined below. As part of their contractual relations, the parties shall undertake to comply with the applicable regulations on personal data processing and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 which is applicable from 25 May 2018 (hereinafter " the General Data Protection Regulation ").

II. Description of the processing being subcontracted out

The processor is authorized to process, on behalf of the controller, the necessary personal data for providing Technology Expense Management tools and services. The nature of operations carried out on the data is Data collection from technology providers (carrier, vendors…), data collection from software agents located on devices, data collection from the controller or its clients (HR data, accounting data, technical data…), data conversion, data integration in data gases, analytics production, KPI production, dashboard production, from this data. The purpose of the processing is good cost and technical management of the controller’s (or its client’s) technical resources. The personal data processed are the following: Full name, EID, position, email, Call Data Records (CDR’s) for voice, text and data usage, data usage per application, country from where the data is used, device information. All categories of person are involved. To perform the service covered herein, the controller shall provide the processor with the following necessary information: access to carrier/vendor billing information, access to RH files, CDR’s from carriers or PABX’s, access to mobile device CDR’s. The data is hosted, according to controller’s choice and instructions, either in E.U., or outside of E.U.. Data is then located in the datacenters of the chosen region.

III. Duration of the contract

This contract duration is aligned with the service contract duration subscribed by the controller.

IV. Processor's obligations with respect to the controller

The processor shall undertake to:

1. Process the data solely for the purpose(s) subject to the sub -contracting

2. Process the data in accordance with the documented instructions from the controller. Where the processor considers that an instruction infringes the General Data Protection Regulation or of any other legal provision of the Union or of Member States bearing on data protection, it shall immediately inform the controller thereof. Moreover, where the processor is obliged to transfer personal data to a third country or an international organization, under Union law or Member State law to which the processor is subject, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3. Guarantee the confidentiality of personal data processed hereunder.

4. Ensure that the persons authorized to process the personal data hereunder: (i) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (ii) receive the appropriate personal data protection training.

5. Take into consideration, in terms of its tools, products, applications or services, the principles of data protection by design and by default.

6. Sub -contracting
   The processor is authorized to engage the entities AWS (hosting), Azure (hosting), NTT Europe (hosting), Oracle (Database maintenance), StoreData (Storage maintenance), Zendesk (customer service ticket storage), (hereinafter the "sub-processor") to carry out the processing activities specified in parenthesis. Where the processor recruits other sub -processors: The sub-processor is obliged to comply with the obligations hereunder on behalf of and on instructions from the controller. It is the initial processor's responsibility to ensure that the sub-processor provides the same sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing meets the requirements of the General Data Protection Regulation. Where the sub-processor fails to fulfil its data protection obligations, the initial processor remains fully liable with regard to the controller for the sub-processor's performance of its obligations.

7. Data subjects' right to information
   It is the controller's responsibility to inform the data subjects concerned by the processing operations at the time data are being collected.

8. Exercise of data subjects' rights
   The processor shall assist the controller, insofar as this is possible, for the fulfilment of its obligation to respond to requests for exercising the data subject's rights: right of access, to rectification, erasure and to object, right to restriction of processing, right to data portability, right not to be subject to an automated individual decision (including profiling). The processor must respond, in the name and on behalf of the controller within the periods referred to by the General Data Protection Regulation, to data subjects' requests to exercise their rights, with regard to data covered by the sub-contracting provided for hereunder.

9. Notification of personal data breaches
   The processor shall notify the controller of any personal data breach not later than 72 hours

after having become aware of it and via email. Said notification shall be sent along with any necessary documentation to enable the controller, where necessary, to notify this breach to the competent supervisory authority. Possible option Once the controller has agreed, the processor shall notify the competent supervisory authority, in the name and on behalf of the controller, of the personal data breaches without undue delay and, where feasible, not later than 72 hours after having become aware of them, unless the breach in question is unlikely to result in a risk to the rights and freedoms of natural persons. The notification shall at least: (i) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (ii) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (iii) describe the likely consequences of the personal data breach; (iv) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

10. Assistance lent by the processor to the controller regarding compliance with its obligations. The processor assists the controller in carrying out data protection impact assessments. The processor assists the controller with regard to prior consultation of the supervisory authority.

11. Security measures
The processor undertakes to implement the following security measures:

(i) Data encryption upon collection and transfer to the processor's servers, data restricted to the "agent" application on mobile devices,

(ii) Restriction of access to data through the user interface, on the basis of email/password user authentication and by administration of access rights on the application level, masking of personal data in the application, data access restricted to software support and maintenance teams, restriction of access to production environments and data based on administration of physical and logical access of the host and on securing access to the servers,

(ii a) Architecture is replicated to ensure availability of services, incremental daily backup and full weekly backup to limit data loss in case of a major incident, functional and technical tests for each major software release, application and system supervision, centralized administration of access logs and application logs,

(ii b) Each employee signs a confidentiality agreement (as an addendum to their employment contract)

(iii) Business continuity plan to mitigate any major host incident, PaaS (Platform as a Service) hosting for rapid deployment of new servers,

(iv) Quarterly internal monitoring of the Security Plan.

In the event that the data controller provides personal data to the processor in the form of a file, the data controller is responsible for encrypting this data in accordance with the method defined with the processor.

The data controller is responsible for the accuracy of data provided by file or entered in the HMI by the data controller's administrators.

For the reporting functionality, the data controller is responsible for distribution of reports containing personal data via emails to contacts who are not users of the processor's software.

In the event that the data controller chooses to leverage their own SSO authentication solution, the Client is therefore responsible for user authentication and for the security of their solution.

12. Fate of data.
    At the end of the service bearing on the processing of such data, the processor undertakes to destroy or pseudonymize all personal data in a delay of maximum 12 months. Once destroyed or pseudonymized, the processor must demonstrate, in writing, that this destruction or pseudonymization has taken place.

13. The Data Protection Officer.
    The processor communicates to the controller the name and contact details of its data protection officer (DPO), if it has designated one in accordance with Article 37 of the GDPR.
14. Record of categories of processing activities.
    The processor states that it maintains a written record of all categories of processing activities carried out on behalf of the controller, containing: (i) the name and contact details of the controller on behalf of which the processor is acting, any other processors and, where applicable, the data protection officer; (ii) the categories of processing carried out on behalf of the controller; (iii) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards; (iv) where possible, a general description of the technical and organizational security measures, including inter alia: (a) the pseudonymization and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

15. Documentation.
    The processor provides the controller with the necessary documentation for demonstrating compliance with all of its obligations and for allowing the controller or any other auditor it has authorized to conduct audits, including inspections, and for contributing to such audits.

V. Controller's obligations with respect to the processor.

The controller undertakes to:

1. Provide the processor with the data mentioned in II hereof
2. Document, in writing, any instruction bearing on the processing of data by the processor
3. Ensure, before and throughout the processing, compliance with the obligations set out in the General Data Protection Regulation on the processor's part
4. Supervise the processing, including by conducting audits and inspections with the processor.

Date:

The processor (Saaswedo)	The controller (The Client)
Name	Name
Title	Title
Signature	Signature