DATA PROCESSING AGREEMENT

This Data Processing Agreement, including all its exhibits (this “**DPA**”), is entered into by and between Sagacify S.R.L. incorporated and registered in Belgium with company number 0500.616.505 whose registered office is at 1150 Sint-Pieters-Woluwe, Avenue de Broqueville 12 ("**Skwiz**") and the customer agreeing to these terms (the “**Customer**”) (each, a “**Party**” and, collectively, the “**Parties**”). This DPA forms part of the Agreement (as defined in the recitals below) between Skwiz and Customer. This DPA replaces any data processing agreement or addendum that was previously concluded between the Customer and Skwiz.

This DPA sets out obligations of the Parties with respect to data protection in relation to the Agreement. To the extent of any conflict or inconsistency between the provisions of this DPA (including any exhibits and appendices thereto) and any provision of the Agreement, the provisions of this DPA shall prevail and take precedence over such conflicting or inconsistent provisions in the Agreement.

BACKGROUND

(A) Skwiz provides services as set out in section 2.1 of the Skwiz Terms and Conditions (hereinafter “**Services**”). In providing these Services, Skwiz may process personal data (as defined below) on behalf of Customer.

(B) The Parties have concluded a main agreement regarding these Services (hereinafter referred to as, "**Agreement**"), which they now wish to supplement in respect of their data processing obligations under Applicable Data Protection Law (as defined hereunder).

(C) This DPA sets out the additional terms, requirements and conditions on which Skwiz will process Personal Data when providing services under the Agreement.

AGREED TERMS

1. Definitions

1.1 The terms "**controller**", "**processor**", "**data subject**", "**personal data**", "**processing**" (and "**process**") and "**special categories of personal data**" have the meanings given in Applicable Data Protection Law;

1.2 "**Applicable Data Protection Law**" means:

(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, and repealing Directive 95/46/EC ("**General Data Protection Regulation**" or "**GDPR**");

(ii) Directive 2002/58/EC on the protection of privacy in the context of electronic communications (the "**ePrivacy Directive**");

(iii) any and all applicable national data protection laws in EEA member states made under, pursuant to, or that apply in conjunction with any of (i) or (ii) above;

in each case as may be amended or superseded from time to time;

1.3 "**European Economic Area**" or "**EEA**" means the Member States of the European Union, plus Norway, Iceland and Lichtenstein.

2. Relationship of the parties

2.1 The Customer (the controller) appoints Skwiz as a processor to process the personal data described in Annex I: Data Processing Description / that is the subject of this DPA (the "**Data**"). Each Party shall comply with the obligations that apply to it under Applicable Data Protection Law.

3. Prohibited data

3.1 The Customer shall not disclose (and shall not require any data subject to disclose) any special categories of personal data to Skwiz for processing.

4. Purpose limitation

4.1 Skwiz shall process the Data as a processor and strictly in accordance with the documented instructions of Customer (the "**Permitted Purpose**"), except where otherwise required by any EEA member state law applicable to Skwiz.

4.2 Notwithstanding section 4.1, Skwiz shall only process the Data for its own secondary purposes, namely for the purposes of quality testing or improving the services, insofar as this is permitted under Applicable Data Protection Law. In such a case, as the controller of the personal data concerned, Skwiz will take the necessary measures and precautions under Applicable Data Protection Law.

4.3 Skwiz shall immediately inform Customer if it becomes aware that Customer's processing instructions infringe Applicable Data Protection Law (but without obligation to actively monitor Customer's compliance with Applicable Data Protection Law).

5. Instructions by Customer

5.1 Customer may give specifications to such instructions provided in the Agreement and this DPA as well as further instructions. Any further instructions that go beyond the instructions contained in this DPA or the Agreement shall be within the subject matter of the Agreement and this DPA. Instructions shall be given in writing.

6. International transfers

6.1 Skwiz shall not transfer the Data (nor permit the Data to be transferred) outside of the EEA unless the transfer is to a country, region or sector that has been recognized by the European Commission as providing an adequate level of protection for personal data in accordance with Applicable Data Protection Law.

6.2 The Parties agree that if the Data is being transferred to, stored by, or accessed by Skwiz in a country or region, or by a sector, outside the EEA that is not deemed adequate by the European Commission, such transfer of personal data shall be subject to the Standard Contractual Clauses, unless Skwiz demonstrates that it has put in place other appropriate safeguards in accordance with Applicable Data Protection Law.

7. Confidentiality of processing

7.1 Skwiz shall ensure that any person that it authorises to process the Data (including Skwiz's staff, agents and subcontractors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Data who is not under such a duty of confidentiality. Skwiz shall ensure that all Authorised Persons process the Data only as necessary for the Permitted Purpose.

8. Security

8.1 Skwiz shall implement and maintain appropriate technical and organisational measures to protect the Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Data (a "**Security Incident**"). Such measures shall have regard to 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.

8.2 At a minimum, such measures shall include the measures identified in the Annex II "**Technical and Organizational Security Measures**" to this DPA.

9. Security Incidents

9.1 Upon becoming aware of a Security Incident, Skwiz shall inform Customer without undue delay and shall provide all such timely information and cooperation as Customer may reasonably require in order for Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Skwiz shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Customer informed of all developments in connection with the Security Incident.

10. Sub processing

10.1 Skwiz shall not subcontract any processing of the Data to a third party sub processor (a "**Sub-processor**") without the prior written consent of Customer.

10.2 Notwithstanding this, Customer consents to Skwiz engaging Sub-processors to process the Data provided that: (i) Skwiz provides at least 15 days' prior notice of the addition or removal of any sub processor (including details of the processing it performs or will perform), which may be given by posting details of such addition or removal at the following URL: https://skwiz.ai/subprocessor-list (ii) Skwiz imposes data protection terms on any sub processor it appoints that protect the Data to the same standard provided for by this DPA; and (iii) Skwiz remains fully liable for any breach of this DPA that is caused by an act, error or omission of its Sub-processors.

10.3 If Customer refuses to consent to Skwiz's appointment of a Sub-processor on reasonable grounds relating to the protection of the Data, then either Skwiz will not appoint the Sub-processor or Customer may elect to suspend or terminate this DPA without penalty.

11. Cooperation and data subjects' rights

11.1 Skwiz shall provide all reasonable and timely assistance to Customer (at its own expense) to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Skwiz, Skwiz shall promptly inform Customer providing full details of the same.

12. Data Protection Impact Assessment

12.1 Upon Customer's request, Skwiz shall provide Customer with all reasonable and timely assistance as Customer may require in order to conduct a data protection impact assessment in accordance with Applicable Data Protection Law including, if necessary, to assist Customer to consult with its relevant data protection authority.

13. Deletion or return of Data

13.1 Upon termination or expiry of the Agreement, Skwiz shall (at Customer's election) destroy or return to Customer all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a Sub-processor for processing).

13.2 This requirement shall not apply to the extent that Skwiz is required by any EU (or any EEA member state) law to retain some or all of the Data, in which event Skwiz shall isolate and protect the Data from any further processing except to the extent required by such law until deletion is possible.

14. Audit and verification of compliance

14.1 Upon Customer's request, Skwiz shall make available to Customer all information necessary to demonstrate compliance with this Clause.

14.2 Skwiz shall permit Customer (or its appointed third party auditors) to audit Skwiz's compliance with this DPA, and shall make available to Customer all information, systems and staff necessary for Customer (or its third party auditors) to conduct such audit. Skwiz acknowledges that Customer (or its third party auditors) may enter its premises for the purposes of conducting this audit, provided that Customer gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Skwiz's operations. Customer will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) Customer believes a further audit is necessary due to a Security Incident suffered by Skwiz.

Annex I
Data Processing Description

In the context of the DPA, Skwiz performs the processing operations on the personal data listed below:

Data submitted by the user of the Skwiz Software
Any personal data contained in the documents submitted to the Skwiz software. **Documents that can be submitted by the Customer to the Skwiz Software can be, but are not limited to: invoices, receipts, purchase orders, packing lists, quotes, custom forms, contracts, medical invoices, medical certificates, identity papers, badges.**

The Personal Data will be used to perform the Services as set out in the Agreement. In particular, the object of the processing is the following:

Nature and purpose for processing
Extraction, processing, interpretation and structuring of information from various types of documents submitted by the Customer.
Locations where data will be processed
Skwiz is a cloud-application and the Data will be stored in the cloud. Our data centres are managed by Amazon AWS and are exclusively situated in the EU / EEA.
Duration of processing activities
Any data submitted by the Customer is retained for 2 months following submission (unless configured or agreed differently with the Customer).

Annex II
Technical and Organizational Security Measures

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measures of pseudonymisation and encryption of personal data	No pseudonymisation is performed. All the data is encrypted at rest (AWS storage with keys managed through KMS) and in transit (https).
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	The solution is working in high availability on 3 separate geographical availability zones. System and service are always duplicated in 2 zones and can switch to the third one if one zone is not working properly. All data is encrypted in transit (https) and at rest (AES256) with a document signing performed at AWS S3 level.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	The solution is always deployed on 2 of 3 availability zones. In the event of an incident, the load is balanced on the third zone to ensure fast recovery of the system.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Periodical batteries of tests through CI/CD, tests for each code update, AWS Inspector automatically check security patches and new versions of all running systems.
Measures for user identification and authorisation	Passwords and api keys are hashed / salted and never stored in clear.
Measures for the protection of data during transmission	Data is always encrypted during transmission (https).
Measures for the protection of data during storage	Data is always encrypted at rest through AWS S3 with encryption keys managed through AWS KMS.
Measures for ensuring physical security of locations at which personal data are processed	Security provided by data centres managed by AWS.
Measures for ensuring events logging	Logging system using AWS CloudWatch and ELK stack.
Measures for ensuring system configuration, including default configuration	Infrastructure as code. All configs of all systems are version controlled and backed up.
Measures for internal IT and IT security governance and management	Training, constant monitoring and logs monitoring, periodic vulnerability assessments, access control, predefined incident response plan.
Measures for certification/assurance of processes and products	All developments made on top of standard and open source libraries.

Measures for ensuring data minimisation	The raw documents are fully stored during the minimum necessary period to support the extraction / reviewing process, but only the specific information required to be extracted are stored in the databases.
Measures for ensuring data quality	No specific measures, customers are responsible for the quality of the sent data.
Measures for ensuring limited data retention	Data is stored during the minimum necessary period to support the extraction / reviewing process and is then deleted.
Measures for ensuring accountability	Roles and responsibilities of the Skwiz team are clearly defined. Quality of the solution is ensured through advanced monitoring.
Measures for allowing data portability and ensuring erasure	Data can be transferred or asked to be deleted anytime on user request. Data is also automatically deleted after the retention period.