COVVE SCAN SERVICE AGREEMENT

PARTIES

(1) **COVVE VISUAL NETWORK LIMITED**, a limited liability company, duly organised and validly existing under the laws of the Republic of Cyprus, with registration number HE 286317, and corporate registered office address located at: 8, Michalaki Karaoli street, Anemomylos Building, 4th Floor, 1095, Nicosia, Cyprus **(Supplier)**

(2) **The "Customer"**

BACKGROUND

(A) The Supplier has developed a mobile application and platform under the name Covve Scan which it makes available as a service to customers for the purpose of digitising business cards (the "**Covve Scan Application**").

(B) The Customer wishes to obtain from the Supplier the Services (as the term is defined below) in the course of its business operations.

(C) The Supplier has agreed to provide its Services and the Customer has agreed to take such Services subject to the terms and conditions of this agreement.

AGREED TERMS

1. Interpretation

1.1 The definitions and rules of interpretation in this clause apply in this agreement.

Account Manager: a person responsible for the management of a Customer's access to the Services, as he/she is to be designated by the Supplier to the Customer.

Business Day: a day other than a Saturday, Sunday or public holiday in Cyprus, when banks in Cyprus are open for business.

Confidential Information: information that is proprietary or confidential and is either clearly labelled as such or identified as Confidential Information in clause 8.5 or clause 8.6.

Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing: as defined in the Data Protection Legislation.

Customer Data: the data inputted by the Customer or the Supplier on the Customer's behalf for the purpose of using the Services or facilitating the Customer's use of the Services and any data generated by, or derived from the Customer's use of the Services, whether hosted or stored within the Services or elsewhere.

Data Protection Legislation: the GDPR, the Cyprus Data Protection legislation and all other legislation and regulatory requirements in force from time which apply to a party relating to the use of personal data.

Data Processing Agreement: the Data Processing Agreement to be signed between the Supplier (as the processor) and the Customer (as the controller) as per Schedule 2 to this Agreement.

Data Subject: means the individual to whom Personal Data relates.

GDPR: means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as amended from time to time.

Fees: the Fees payable by the Customer to the Supplier as set out in clause 7.

Initial Term: the initial term of this agreement as set out in clause 12.

Renewal Period: the period described in clause 12.1.

Services: the services provided by the Supplier to the Customer via the Software, as such services are described in Schedule 1 of this Agreement.

Software: the Covve Scan Application and/or any other online or mobile software application provided by the Supplier to the Customer as part of the Services.

Supplier's Privacy Policy: The privacy policy found at https://covve.com/legal/covve/consumer/covve-privacy

Term: has the meaning given in clause 11.1 (being the Initial Term together with any subsequent Renewal Periods)

Virus: any thing or device (including any software, code, file or programme) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme or data (whether by re-arranging, altering or erasing the programme or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

Vulnerability: a weakness in the computational logic (for example, code) found in software and hardware components that when exploited, results in a negative impact to the confidentiality, integrity, or availability, and the term Vulnerabilities shall be construed accordingly.

1. Grant of licence

1.1 Subject to the terms and conditions of this agreement and subject to payment by the Customer of the Fees, the Supplier hereby grants to the Customer a non-exclusive, non-transferable right, without the right to grant sublicences, to use the Software during the Term solely for the Customer's internal business operations.

2. Services

2.1 The Supplier shall, during the Term, provide the Services to the Customer subject to the terms of this agreement.

The Supplier shall use commercially reasonable endeavours to make the Services available 24 hours a day, seven days a week, except for:

(a) scheduled maintenance in which case the Supplier shall give the Customer at least 10 days notice; and

emergency maintenance required for the resolution of an issue or for maintaining the security of the solution.

3. Customer data

3.1 The Customer shall own all right, title and interest in and to all of the Customer Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of all such Customer Data.

3.2 Both parties will comply with all applicable requirements of the Data Protection Legislation.

3.3 The Parties shall comply with the Data Processing Agreement in Schedule 2, which forms an integral part of this Agreement and which sets out the scope, nature and purpose of processing by the Supplier, the duration of the processing and the types of personal data and categories of data subject.

3.4 The parties acknowledge that:

(a) if the Supplier processes any personal data on the Customer's behalf when performing its obligations under this agreement, the Customer is the Controller and the Supplier is the Processor for the purposes of the Data Protection Legislation.

(b) the personal data may be transferred or stored outside the EEA or the country where the Customer is located in order to carry out the Services and the Supplier's other obligations under this agreement as set out in the DPA in Schedule 2.

3.5 Without prejudice to the generality of clause 4.2, the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the personal data to the Supplier for the duration and purposes of this agreement so that the Supplier may lawfully use, process and transfer the personal data in accordance with this agreement on the Customer's behalf.

3.6 Each party shall ensure that it has in place appropriate technical and organisational measures, to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures. Specifically, the Supplier will put in place the technical and organisational measures set out in Schedule 3.

3.7 The parties acknowledge that, separately from the Personal Data processed by the Supplier as Processor on the Customer's behalf under the Data Processing Agreement, the Supplier processes certain Personal Data relating to the Customer's Authorised Users — including account, authentication, support, device and usage data — as a Controller in its own right, for the purposes of providing, securing, supporting and improving the Services. Such processing is described in the Supplier's Privacy Policy.

4. Supplier's obligations

4.1 The Supplier undertakes that the Services will be performed substantially in accordance with the terms and conditions of this agreement and with reasonable skill and care.

4.2 The Supplier:

(a) does not warrant that:

(i) the Customer's use of the Software or the Services will be uninterrupted or error-free;

(ii) that the Software and the Services to be provided to the Customer will meet the Customer's requirements;

(iii) the Software or the Services will be free from Vulnerabilities;

(b) is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Services may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

4.3 This agreement shall not prevent the Supplier from entering into similar agreements with third parties, or from independently developing, using, selling or licensing products and/or services which are similar to those provided under this agreement.

4.4 The Supplier warrants that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under this agreement.

4.5 The Supplier will, as part of the Services and at no additional cost to the Customer, provide the Customer with a high priority support, as follows:

(a) For any critical issues (e.g. the Services are unavailable), the Account Manager will respond to the Customer within 2 hours, from 7am – 7pm EET, 7 days a week; and

(b) A lead engineer will be assigned to the issue and will commence investigation as a first priority from 8am – 5pm EET, during Business Days (the "**Business Hours**").

5. Customer's obligations

The Customer shall:

(a) provide the Supplier with:

(i) all necessary co-operation in relation to this agreement; and

(ii) all necessary access to such information as may be required by the Supplier;

in order to provide the Services, including but not limited to Customer Data, security access information and configuration services;

(b) without affecting its other obligations under this agreement, comply with all applicable laws and regulations with respect to its activities under this agreement;

(c) carry out all other Customer responsibilities set out in this agreement in a timely and efficient manner. In the event of any delays in the Customer's provision of such assistance as agreed by the parties, the Supplier may adjust any agreed timetable or delivery schedule as reasonably necessary;

(d) obtain and shall maintain all necessary licences, consents, and permissions necessary for the Supplier, its contractors and agents to perform their obligations under this agreement, including without limitation the Services;

(e) be, to the extent permitted by law and except as otherwise expressly provided in this agreement, solely responsible for procuring, maintaining and securing its mobile and/or network connections and telecommunications links from its devices and/or systems to the

Supplier's data centres, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Customer's network connections or telecommunications links or caused by the internet.

5.2 The Customer shall not access, store, distribute or transmit any Viruses, or any material during the course of its use of the Services.

5.3 The Customer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Services and, in the event of any such unauthorised access or use, promptly notify the Supplier.

5.4 The rights provided under this clause 6 are granted to the Customer only and shall not be considered granted to any subsidiary or holding company of the Customer.

6. Charges and payment

6.1 The Fees chargeable for the Service will be agreed between Covve and the Customer on submission of the first Order Form.

6.2 The Customer shall settle the invoice within thirty (30) days from the date of its issue. Failure to do so, it will result to an interest which will accrue on a daily basis on such due amounts at an annual rate equal to 3%, commencing on the due date and continuing until fully paid.

6.3 All amounts and fees stated or referred to in this Agreement are exclusive of value added tax which, wherever applicable, shall be added accordingly to COVVE’s invoice(s) at the appropriate rate.

7. Proprietary rights

7.1 The Customer acknowledges and agrees that the Supplier and/or its licensors own all intellectual property rights in the Software and the Services. Except as expressly stated in this agreement, this agreement does not grant the Customer any rights to, under or in, any patents, copyright, database right, trade secrets, trade names, trade marks (whether registered or unregistered), or any other rights or licences in respect of the Software and the Services.

7.2 The Supplier confirms that it has all the rights in relation to the Software that are necessary to grant all the rights it purports to grant and to provide the Services under, and in accordance with, the terms of this agreement.

8. Confidentiality

8.1 Each Party may be given access to Confidential Information from the other party in order to perform its obligations under this agreement. A party's Confidential Information shall not be deemed to include information that:

(a) is or becomes publicly known other than through any act or omission of the receiving party;

(b) was in the other party's lawful possession before the disclosure;

(c) is lawfully disclosed to the receiving party by a third party without restriction on disclosure; or

(d) is independently developed by the receiving party, which independent development can be shown by written evidence.

8.2 Subject to clause 8.5, each party shall hold the other's Confidential Information in confidence and not make the other's Confidential Information available to any third party, or use the other's Confidential Information for any purpose other than the implementation of this agreement.

8.3 Each party shall take all reasonable steps to ensure that the other's Confidential Information to which it has access is not disclosed or distributed by its employees or agents in violation of the terms of this agreement.

8.4 A party may disclose Confidential Information to the extent such Confidential Information is required to be disclosed by law, by any governmental or other regulatory authority or by a court or other authority of competent jurisdiction, provided that, to the extent it is legally permitted to do so, it gives the other party as much notice of such disclosure as possible and, where notice of disclosure is not prohibited and is given in accordance with this clause 8.4, it takes into account the reasonable requests of the other party in relation to the content of such disclosure.

8.5 The Customer acknowledges that details of the Services, and the results of any performance tests of the Services, constitute the Supplier's Confidential Information.

8.6 The Supplier acknowledges that the Customer Data is the Confidential Information of the Customer.

8.7 The above provisions of this shall survive termination of this agreement, however arising.

9. Indemnity

9.1 The Customer shall defend, indemnify and hold harmless the Supplier against claims, actions, proceedings, losses, damages, expenses and costs (including without limitation court costs and reasonable legal fees) arising out of or in connection with the Customer's use of the Services, provided that:

(a) the Customer is given prompt notice of any such claim;

(b) the Supplier provides reasonable co-operation to the Customer in the defence and settlement of such claim, at the Customer's expense; and

(c) the Customer is given sole authority to defend or settle the claim.

9.2 The Supplier shall defend the Customer, its officers, directors and employees against any claim that the Customer's use of the Software and the Services in accordance with this agreement infringes any European patent effective as of the Effective Date, copyright, trade mark, database right or right of confidentiality, and shall indemnify the Customer for any amounts awarded against the Customer in judgment or settlement of such claims, provided that:

(a) the Supplier is given prompt notice of any such claim;

(b) the Customer provides reasonable co-operation to the Supplier in the defence and settlement of such claim, at the Supplier's expense; and

(c) the Supplier is given sole authority to defend or settle the claim.

10. Limitation of liability

10.1 Except as expressly and specifically provided in this agreement:

(a) the Customer assumes sole responsibility for results obtained from the use of the Services by the Customer, and for conclusions drawn from such use. The Supplier shall have no liability for any damage caused by errors or omissions in any information, instructions or scripts provided to the Supplier by the Customer in connection with the Services, or any actions taken by the Supplier at the Customer's direction;

(b) all warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from this agreement; and

(c) the Services are provided to the Customer on an "as is" basis.

10.2 Nothing in this agreement excludes the liability of the Supplier:

(a) for death or personal injury caused by the Supplier's negligence; or

(b) for fraud or fraudulent misrepresentation.

10.3 Subject to clause 10.1 and clause 10.2:

(a) the Supplier shall not be liable whether in tort (including for negligence or breach of statutory duty), contract, misrepresentation, restitution or otherwise for any loss of profits, loss of business, depletion of goodwill and/or similar losses or loss or corruption of data or information, or pure economic loss, or for any special, indirect or consequential loss, costs, damages, charges or expenses however arising under this agreement; and

(b) the Supplier's total aggregate liability in contract (including in respect of the indemnity at clause 9.2), tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise, arising in connection with the performance or contemplated performance of this agreement shall be limited to the total Fees paid for the Services.

11. Term and termination

11.1 This agreement shall, unless otherwise terminated as provided in this clause 12, commence on the date of the first order form that is submitted (whether using the order form in Schedule 4 or by other means) (“**Effective Date”)** and shall continue for a period of 12 months (**Initial Term**) and, thereafter, this agreement shall be automatically renewed for successive periods of 12 months (each a **Renewal Period**), unless:

(a) either Party notifies the other that it wishes to terminate the agreement, in writing, at least 30 days before the end of the Initial Term or any Renewal Period, in which case this agreement shall terminate upon the expiry of the applicable Initial Term or Renewal Period; or

(b) otherwise terminated in accordance with the provisions of this agreement;

and the Initial Term together with any subsequent Renewal Periods shall constitute the **Term**.

11.2 The Customer may terminate this agreement at any time on no less than 90 days prior written notice to the Supplier.

11.3 Without affecting any other right or remedy available to it, either party may terminate this agreement with immediate effect by giving written notice to the other party, if:

(a) the Customer fails to pay any amount due under this agreement on the due date for payment and remains in default not less than 60 days after being notified in writing to make such payment;

(b) the other party commits a material breach of any other term of this agreement which breach is irremediable or if such breach is remediable fails to remedy that breach within a period of 15 days after being notified in writing to do so;

(c) the other party repeatedly breaches any of the terms of this agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms of this agreement;

11.4 On termination of this agreement for any reason:

(a) all licences granted under this agreement shall immediately terminate and the Customer hall immediately cease all use of the Software and the Services;

(b) the Supplier may destroy or otherwise dispose of any of the Customer Data in its possession, unless the Supplier receives, no later than ten days after the effective date of the termination of this agreement, a written request for the delivery to the Customer of the then most recent back-up of the Customer Data. The Supplier shall use reasonable commercial endeavours to deliver the back-up to the Customer within 30 days of its receipt of such a written request, provided that the Customer has, at that time, paid all fees and charges outstanding at and resulting from termination (whether or not due at the date of termination). The Customer shall pay all reasonable expenses incurred by the Supplier in returning or disposing of Customer Data; and

(c) any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the agreement which existed at or before the date of termination shall not be affected or prejudiced.

12. Force majeure

The Supplier shall have no liability to the Customer under this agreement if it is prevented from or delayed in performing its obligations under this agreement, or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control, including, without limitation, strikes, lock-outs or other industrial disputes, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors, provided that the Customer is notified of such an event and its expected duration.

13. Notices

13.1 Any notice required to be given under this agreement shall be in writing and shall be delivered by hand or delivery post to the other party at its address set out in this agreement, or such other address

as may have been notified by that party for such purposes, or sent by email or by fax to the other party's respective email address or fax number as set out in this agreement.

SUPPLIER

Address: Covve Visual Network Limited, 8, Michalaki Karaoli street, Anemomylos Building, 4th Floor, 1095, Nicosia, Cyprus

Email address: admin@covve.com

CUSTOMER

Customer contact details to be provided by the Customer to Covve on submission of the first order form.

13.2 A notice delivered by hand shall be deemed to have been received when delivered (or if delivery is not in business hours, at 9 am on the first business day following delivery). A notice sent by fax shall be deemed to have been received at the time of transmission (as shown by the timed printout obtained by the sender) and a notice sent by email shall be deemed to have been received at the time sent by the other party.

14. Governing law

This agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of the Republic of Cyprus.

15. Jurisdiction

Each party irrevocably agrees that the courts of the Republic of Cyprus shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this agreement or its subject matter or formation (including non-contractual disputes or claims).

This Agreement has been entered into on the Effective Date.

Schedule 1

DESCRIPTION OF SERVICES TO BE PROVIDED VIA THE COVVE SCAN APPLICATION

Provision, through the App Store and Play Store, of the latest version of the “Business card scanner by Covve” mobile application on iOS and Android. The latest version available on the App Store and Play store will be provided, as-is, with no modifications for the customer.

The “Business Unlimited” plan will be provided. The application’s core functionalities include:

a) Taking a photograph of a business card and automatically transcribing the card’s details into digital format
b) Automatic recognition of multiple languages
c) Enabling users to add notes and tags
d) Enabling users to share previously scanned business cards with other people
e) Enabling users to save previously-scanned business cards to their phone’s address book
f) Enabling users to export previously-scanned business cards

As scanned card data is only stored on user mobile devices, backup and restore of data must be enabled within the Application by each user.

Schedule 2

DATA PROCESSING AGREEMENT

regarding the engagement as Processor pursuant to Article 28 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as "**GDPR**")

between

The Customer, referred to as "**Controller**"

- and -

The Supplier, referred to as "**Processor"**

hereinafter collectively referred to as the "**Parties**".

1. This Data Processing Agreement is entered into between the Parties in the context of the provision of Services provided by the Processor to the Controller via the Covve Scan Application pursuant to the terms of the relevant Software as a Service Agreement (referred to as the "**SaaS Agreement**"~~)~~;

2. Personal data specified in paragraph 4 hereof (hereinafter referred to as "**Data**") will be processed by the Processor from the "Effective Date" as defined in the SaaS Agreement for the sole purpose of the SaaS Agreement execution. Data will continue to be processed until the end of the said SaaS Agreement, unless otherwise directly instructed by the Controller.

3. The Controller engages the Processor to provide Services (as specified in Schedule 1 of the SaaS Agreement) to the Controller.

   Data may also be processed in order to comply with disclosure requirements arising by virtue of operation of law. In this case the Processor shall notify the Controller in advance about such requirements as set forth in paragraph 5 below.

   Processor staff will not access the data, unless this is necessary in order to improve the quality of the Services or where they are obliged to do so in order to comply with a legal obligation, or unless otherwise instructed to do so by the Controller.

   Some features use AI, provided by Microsoft Azure OpenAI, to (i) transcribe your voice notes, (ii) summarise notes you enter, and (iii) summarise publicly available information about a contact at your request. These features are assistive only, outputs are always shown to you to review and edit, and are never used for automated decision-making or profiling. Your data is not used to train AI models and is not retained by the AI service beyond processing your request. AI outputs may be incomplete or inaccurate.

4. The following categories of Data of the following categories of data subjects will be processed:

Categories of data subjects	Categories of Data
Any person that the Controller sends to the Processor for the purposes of entering as a lead into Covve. This includes scanning business card, QR and manual or voice entry.	Image of the person's business card with all data mentioned therein such as name, surname, company, job title, phone number and email as well as notes and additional information entered by the user; voice recordings and their transcriptions; and information about the contact retrieved from publicly available sources at the Controller's request (e.g. professional background, awards, news).
Any person within the Controller's organisation making use of the applications provided by the Processor	Application usage data collected purely for the purpose of improving the service and troubleshooting issues, IP address in system logs
Representatives of the Controller communicating with the Processor's support team for the purposes of support	Name, surname, email and telephone number

5. The Processor is obliged to adhere to all applicable data privacy regulations. In particular, the following obligations apply:

    a. The Processor processes the Data only on documented instructions from the Controller, including with regard to transfers of Data to a third country or an international organisation, unless required to do so by European Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Unless otherwise directly instructed by the Controller, this Agreement constitutes such written instruction of the Controller for the processing of Data. The Processor ensures that access to Data is granted to persons under its authority only on a need to know basis and such persons authorised to process Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. In particular Processor‘s employees as well as any Sub-processors or their employees, shall have committed themselves to confidentiality or shall be under an appropriate statutory obligation of confidentiality.

    b. The Processor takes all measures required pursuant to Article 32 of the GDPR.

    The Processor shall engage sub-processors for the provision of the Services and the Controller hereby approves the sub-processors listed in the table below:

Name	Place of processing	Purpose of Use
Microsoft	Europe	Microsoft Azure is used for the hosting of the entire solution.
F5	Europe	F5 provides Web Application Firewall services for the increased security of the solution.
Google Inc	Europe	To provide analysis services used in the process of scanning and storage for user leads/contacts and backups.

The Processor shall inform the Controller of any intended changes concerning the addition or replacement of other sub-processors, thereby giving the Controller the opportunity to object to such changes. The Controller may object to the addition or replacement of sub-processors within 7 days after the Processor's notification of the intended change. If the Controller neither approves nor objects within such period, the respective sub-processor shall be deemed as approved. The Controller shall not unreasonably object to any intended change.

c. Where the Processor engages a sub-processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in this Agreement shall be imposed on the sub-processor. Where the sub-processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the sub-processor's obligations.

d. Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights pursuant to Chapter III of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**").

e. Further, the Processor assists the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the Processor. If the Processor needs any information or other assistance from the Controller to make the processing of Data in line with GDPR, the Processor shall directly inform the Controller about that.

f. At the choice of the Controller, the Processor shall delete or return all the Data to the Controller after the termination of the SaaS Agreement or the end of the provision of Services relating to Data processing and shall delete existing copies unless European Union and/or Member State law requires storage of the Data.

g. The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other European Union or Member State data protection provisions.

h. The Processor guarantees that it implemented appropriate technical and organisational measures to ensure that processing of Data will meet GDPR requirements and data subjects' rights will be protected as well as to ensure confidentiality, integrity and availability of Data processed on behalf of the Controller. Namely, the Processor deployed technical security measures as set out in Schedule 3.

i. As applicable, the Standard Contractual Clauses and any corresponding modules as set out in Schedule 4 will apply to this Agreement.

6. This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of the Republic of Cyprus.

Schedule 3

TECHNICAL AND ORGANIZATIONAL MEASURES

Measures of pseudonymisation and encryption of personal data	• All data is encrypted both in transit (TLS, between client and server and between servers and databases) and at rest (both live system and all backups).
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	• Staff responsible for the development, implementation and maintenance of Covve's information security program; • Continuous uptime monitoring of all systems; • Data security controls including logical segregation of data, role-based access and monitoring; • Network security controls including isolated VNETs, firewalls and user authentication at all necessary levels; • Automatic and continuous vulnerabilities scanning, patch management and threat protection, both on environments/servers and on application-level code; • Highly available, auto-scaling and redundant server infrastructure and geo-replicated databased provided by Azure; • Use of best practices for the management of keys and secrets within the environment without human intervention; • Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from emergency situations or disasters.
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	• Incident management procedures designed to allow Covve to detect, investigate, respond to, and mitigate incidents; • Continuous geo-redundant backups of all data with RTO and RPO of 15 minutes.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	• Annual 3rd party penetration test, currently by Census Labs; • Annual 3rd party holistic privacy and security, currently by Cybervadis; • Quarterly review by internal management for compliance to policies and procedures
Measures for user identification and authorisation	• Logical access controls based on the least privilege basis; • Use of unique IDs and passwords for all users to all systems; • Password controls designed to manage and control password strength; • Multi-factor authentication, where available, must always be used; • Use of OAuth2 for user authentication; • Restricted remote access to production systems using best industry practices; • Restricted access to productions systems to select senior team members (specifically, access is only provided to Covve's technical co-founder, the CTO and head of backend engineering).
Measures for the protection of data during transmission	• All data is encrypted in transit (TLS, between client and server and between servers and databases).
Measures for the protection of data during storage	• All data is encrypted at rest (both live system and all backups).

Measures for ensuring physical security of locations at which personal data are processed	• All systems and data reside on Microsoft Azure and Google data centers in Europe. Details on security measures and environmental guards can be found here:
	  ○ Azure: https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security
	  ○ Google: https://www.google.com/about/datacenters/data-security/
	• Data is redundantly stored in disparate geographic locations;
	• Office locations from which authorised employees may access the systems are protected by 24 hour staffed reception/security and are accessed via individually-assigned keys/badges. 3rd parties are escorted in the facilities and access is logged.

Measures for ensuring events logging	• Systems, infrastructure and network monitoring are achieved through Azure Defender as well as custom network monitoring alerts; • Access to business applications used by staff is logged through the respective application where applicable.
Measures for ensuring system configuration, including default configuration	• All deployed systems use configuration-as-code and are immutable after deployment.

Measures for internal IT and IT security governance and management	• All solutions changes undergo an automated CI/CD process including passing several thousand tests, necessitating code review from an authorised reviewer, deployment and testing to the UAT environment before deployment to production;
	• For all systems patches are identified and in many cases deployed entirely automatically:
	  ○ All mobile applications utilise Github's "Dependabot" to identify patches the moment they are available;
	  ○ Container images are build via automated CI/CD upon every commit. The new images get all updates of all dependencies and base image;
	  ○ Infrastructure-level patching is undertaken by Microsoft through the PaaS offerings.

Measures for certification/assurance of processes and products	• The Covve Information Systems Management System is maintained, reviewed and enforced by Covve's CTO; • Annual 3rd party penetration test, currently by Census Labs; • Annual 3rd party holistic privacy and security audit, currently by Cybervadis; • Quarterly review by internal management for compliance to policies and procedures
Measures for ensuring limited data retention	• Data stored on each user's mobile device is deleted when they delete the Covve Scan app. • Additionally on termination of the Agreement, all data stored on the Processor's servers are deleted within the required time period.

Schedule 4

STANDARD CONTRACTUAL CLAUSES

The Standard Contractual Clauses will apply to any Processing of Personal Data that is

subject to the GDPR. For the purposes of the Standard Contractual Clauses:

a. Module Two will apply in the case of the Processing under this Agreement.

b. Clause 7 of the Standard Contractual Clauses (Docking Clause) does not apply.

c. Clause 9(a) option 1 (Specific prior authorisation) is selected

d. With regard to Clause 17 of the Standard Contractual Clauses (Governing law), the Parties agree that Option 1 will apply and the governing law will be the law of Cyprus.

e. In Clause 18 of the Standard Contractual Clauses (Choice of forum and jurisdiction), the Parties submit themselves to the jurisdiction of the courts of Cyprus.

f. For the Purpose of Annex I of the Standard Contractual Clauses, Schedule 2 (DPA) contains the specifications regarding the parties, the description of transfer, and the competent supervisory authority.

g. For the Purpose of Annex II of the Standard Contractual Clauses, Schedule 3 of this Agreement contains the technical and organizational measures.

h. The specifications for Annex III of the Standard Contractual Clauses, are determined by Schedule 2 (DPA), clause 6(b). The Sub-processor's contact person's name, position and contact details will be provided by Processor upon request.