This Data Processing Agreement ("Agreement") forms part of the Contract for Services ("Principal Agreement") between

Your Company
(the “Company”)

and

iEnterprises Holdings, LLC.

(the “Data Processor”) (together as the “Parties”)

WHEREAS

1. (A) The Company acts as a Data Controller.
2. (B) The Company wishes to subcontract certain Services, which imply the

   processing of personal data, to the Data Processor.

3. (C) The Parties seek to implement a data processing agreement that complies

   with the requirements of the current legal framework in relation to data processing and with 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

4. (D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1. 1.1.1 "Agreement" means this Data Processing Agreement and all Schedules;
2. 1.1.2 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;
3. 1.1.3 "Contracted Processor" means a Subprocessor;

4. 1.1.4 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
5. 1.1.5 "EEA" means the European Economic Area;
6. 1.1.6 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;
7. 1.1.7 "GDPR" means EU General Data Protection Regulation 2016/679;
8. 1.1.8 "Data Transfer" means:
    1. 1.1.8.1 a transfer of Company Personal Data from the

       Company to a Contracted Processor; or

    2. 1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

   in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

9. 1.1.9 "Services" means the _____ services the Company provides.
10. 1.1.10 "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

1. 2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and
2. 2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions.

Data Processing Agreement — Your Company

2.2 The Company instructs Processor to process Company Personal Data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

1. 4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.
2. 4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing
5.1 Processor shall not appoint (or disclose any Company Personal Data to)

any Subprocessor unless required or authorized by the Company.

6. Data Subject Rights

1. 6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
2. 6.2 Processor shall:
    1. 6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and
    2. 6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws

inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

1. 7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
2. 7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

   Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

1. 9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.
2. 9.2 Processor shall provide written certification to Company that it has fully complied with this section 9 within 10 business days of the Cessation Date.

10. Audit rights

1. 10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.
2. 10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the

Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

1. (a) disclosure is required by law;
2. (b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of the European Union.

Appendix A -Technical and Organisational Measures of the Processor pursuant to Article 32 para. 1 of the GDPR

1. Confidentiality guarantee	
1.1 Admission control Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed and used.	
Technical	**Organizational**
Individual user ID	Plant security, porter
Security locks for individual offices	Arrangements for admission by external parties
Introduction of a user master record for each user	Controlled allocation of keys (including access areas)
All servers are hosted in secure data centers that are regularly tested for security.	

1.2 Access control Measures that are suitable for data processing systems (computers) to be used by unauthorized persons.	
Technical	**Organizational**
Login with user name + password	Management of user authorizations (allocation, revocation)
Automatic/manual screen lock (e.g. password required again for login)	Password policy (including special characters, minimum length)
The data is stored encrypted on mobile devices.	Guideline for the use/disposal of data carriers
	Screen Lock Policy
1.3 Access control Measures to ensure that those authorized to use a data processing systemcan only access the data subject of their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.	
Technical	**Organizational**
Authorization concept and introduction of differentiated access levels (for some systems)	Minimum number of administrators
Shredder (min. level 3, cross cut)	Management of user rights by administrators
External document destruction	
Logging of access to applications (input, modification, deletion of data)for some systems	
1.4 Separation control Measures to ensure that data collected for different purposes can beprocessed separately.	
Technical	**Organizational**
Separation of productive and test environment	
Multi-client capability in relevant applications	

1.5 Pseudonymisation The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.	
Technical	**Organizational**
Separation of the allocation data and storage in a separateand secure system (encrypted if possible)	Internal instruction to anonymize/pseudonymize personal data as far as possiblein the event of disclosure or after expiry of the statutory deletion period.
2. Integrity guarantee	
2.1 Transfer control Measures to ensure that personal data cannot be read, copied, modified or removed by unauthorized persons during electronic transmission or during their transport or storage on data media, and that it is possible to verify and establish at which points a transmission of personal data is envisaged by datatransmission equipment.	
Technical	**Organizational**
Encryption, tunnel connection (VPN = Virtual Private Network)	Care in the selection of transport personnel and vehicles
Digital signature	
Email encryption if required	
2.2 Input control Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered into, modified or removed from data processing systems.	
Technical	**Organizational**
Logging the entry, modification and deletion of data	
Automated/manual control of the protocols	
3. Availability and resilience guarantee	

3.1 Availability control Measures to ensure that personal data is protected against accidentaldestruction or loss.	
Technical	**Organizational**
Backup procedure	Backup procedure
Mirroring server hard disks (e.g. RAID procedure)	Separate storage (off-site)
Uninterruptible Power Supply (UPS)	Server rooms not under sanitary facilities
Firewall	Protective socket strips in server rooms
Virus protection	
Fire and fire alarm systems	
Fire extinguishers in the server room	
Server room air-conditioned	
Regular control of system status (monitoring)	
4. Procedures for regular review, assessment and evaluation of the effectiveness of the technical and organizational measures	
4.1 Data protection measures	
Technical	**Organizational**
Data protection management software	Internal/external data protection officer
Central documentation of all policies/procedures on data protection	Employees trained and committed to confidentiality
Regular, annual review of the effectiveness of the technical measures	Regular training of employees on data protection
Privacy-friendly default setting (Art. 25 para. 2 of the GDPR)	Carrying out a privacy impact assessment, if necessary
Careful and confidential treatment of client data	The organization complies with the information obligations pursuant to Art. 13 and 14 of the GDPR
	Processing activities are recorded
4.2 Incident response management	
Technical	**Organizational**

Use and regularly update a firewall	Documented procedure for dealing with security incidents/data breaches
Use and regularly update a spam filter	Documentation of security incidents/data breaches
Use and regularly update a virus scanner	
4.3 Commission control (outsourcing to third parties)	
Technical	**Organizational**
	Selection of the Processor under due diligence aspects (especially with regard to data protection and data security)
	Obligation of the Processor's employees with regard to confidentiality
	Agreement of control rights with the Processor
	Ongoing review of the Processor and its level of protection

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Your Company

Signature _____

Name: _____

Title: _____

Date Signed: _____

iEnterprises Holdings, LLC. (Processor Company)

Signature _____

Name _____

Title _____

Date Signed _____