DATA PROCESSING AGREEMENT

Between

Company name and form
Registered address
trade register information, such as n°, place

Hereinafter referred to as the "**Controller**"

and

iBabs B.V.

De Factorij 33, 1689 AK Zwaag, The Netherlands
Registered at the Dutch Chamber of Commerce under number 60962062

Hereinafter referred to as the "**Processor**"

Hereinafter individually referred to as "**Party**" and collectively referred to as the "**Parties**".

Preamble

On date, the Controller and Processor concluded a contract with regard to the iBabs Licenses (the "**Main contract**").

In the framework of the Main contract, the Processor will Process Personal Data on behalf of the Controller.

The Personal Data Protection Legislation provides that, if the Processing of Personal Data is consigned to a processor, the Processing shall be governed by a contract and that such contract should stipulate certain matters related to the Processing.

This Data Processing Agreement, which forms an integral part of the Main contract, exists to ensure the foregoing.

1. Purpose

The purpose of this agreement is to lay down the provisions governing the relation between the Controller and the Processor in order for both Parties to comply with the obligations provided for by the Personal Data Protection Legislation.

It applies to all Processing activities of Personal Data and to all Personal Data that are Processed by the Processor on behalf of the Controller.

2. Definitions

Personal Data	any information relating to an identified or identifiable natural person ('**Data subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal Data breach	breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed
Personal Data Protection Legislation	As of May 25, 2018, *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) ("**GDPR**") and any delegated and implementing acts related to GDPR
Processing / Process(es) / Processed	any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. Ownership of the data

All Personal Data provided by the Controller to the Processor and which are Processed under the terms of this agreement by the Processor on behalf of the Controller are and shall remain exclusively the property of the Controller, except where the Processor lawfully obtained the same data from another source or obtained the data as a controller.

4. Information about the Processing and contact details of the Processor

Information about the nature and purpose of the Processing, the types of Personal Data Processed and the categories of Data subjects, as well as contact details of the Processor, are specified in **Schedule A** to this agreement.

4. Obligations of the Processor

4.1 Processing of Personal Data

The Processor shall:

- Process the Personal Data only on instructions from the Controller, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject; in the latter 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;
- not Process the Personal Data for any other purposes;
- comply with the Personal Data Protection Legislation;
- at the choice of the Controller, delete or return all the Personal Data to the Controller after the end of the provision of services relating to the Processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data.

4.2 Safeguard of the Personal Data

Taking into account the harm that might result from unauthorized or unlawful Processing or accidental loss, destruction or alteration to Personal Data and to the nature of Personal Data to be protected, the Processor shall use its best endeavours to safeguard the Personal Data from unauthorised or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of Processing and acknowledges that it has implemented at least the technical and organizational security measures specified in **Schedule B** to this agreement to prevent this. These measures shall ensure an appropriate level of security, taking into account the nature of the Processing, the state of technology and the costs of their implementation.

4.3 Restricted access

The Processor shall limit access to the Personal Data to those persons who need to know it to enable the Processor to perform the Processing on behalf of the Controller.

4.4 Confidentiality

The Processor shall ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.5 Location of the processing

The Processing of Personal Data shall take place within the European Union or a third country, or a territory or one or more sectors in such third country, which ensures an adequate level of protection as indicated by the decision of the European Commission taken pursuant to article 25(6) of the Directive or article 45, § 3, of the GDPR.

Any transfer to and Processing in a country outside the European Union that does not ensure an adequate level of protection shall only be undertaken in accordance with the provisions of the Personal Data Protection Legislation, such as e.g. the execution of standard contractual clauses.

4.6 Sub-Processor

The Controller acknowledges and expressly agrees that the Processor may engage third parties as a sub-processor.

In such case the Processor shall:

- contractually impose data protection obligations no less protective than set out in this agreement, in particular obligations providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of the Personal Data Protection Legislation, and
- remain fully liable to the Controller for the sub-processor's compliance with the Processor's obligations under this agreement.

A list of the current sub-processors is attached to this agreement in **Schedule C**. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of sub-processors by the written means that he deems appropriate (including email).

If the Controller objects to the Processing by a new sub-processor, he shall notify the Processor in writing (including email) within 30 calendar days after receipt of the Processor's notice and shall detail the reasonable grounds of his objection. The Controller will in any case not object on unreasonable grounds.

If the Processor is, on a commercially reasonable basis, unable to change the Processing in order to avoid the Processing by such sub-contractor within 60 calendar days as of receipt of the Controller's objection, the Controller may terminate the relevant part of the Main contract for which services cannot be provided without the use of the concerned sub-processor. The Controller shall in that case provide written notice of termination taking into account a notice period 30 days.

4.7 Notification/information obligation in case of a Personal Data breach

The Processor shall notify the Controller, via the email address provided to this end by the latter, of:

- a Personal Data breach, without undue delay and at the latest within 8 hours after becoming aware thereof;
- any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

In case of a Personal Data breach, the Processor shall inform the Controller of the nature of the breach, the nature or type of Personal Data implicated, as the case may be, actions taken or proposed to be taken to remedy or mitigate the effects and minimise the damage and contact details of the data privacy officer or other person who can provide additional information.

The Controller shall notify the Processor immediately about any possible misuse, loss or theft of authorisation credentials, any possible misuse of its accounts or any other security issue.

4.8 Assistance to the Controller with regard to Data subjects' rights

The Controller shall ensure that adequate information about the Processing is provided to Data subjects and shall facilitate the exercise of such rights as provided for by the Personal Data Protection Legislation.

In case a Data subject contacts the Processor to exercise his rights, the Processor will direct the Data subject to the Controller.

Where the Controller requests the Processor's assistance for the fulfilment of its obligations under the Personal Data protections legislation, the Processor will, insofar as this is possible, taking into account the nature of the Processing under this agreement and the information available to the Processor for the Processing activities, provide assistance to the Controller:

- to respond to requests of Data subjects exercising their rights laid down in the Personal Data Protection Legislation; - pursuant to articles 32 to 36 of GDPR.

Such assistance will be provided upon agreement between the Parties and after approval by the Controller of the costs that such assistance will imply for the Processor.

4.9 Data protection impact assessment

The Processor shall provide cooperation and assistance to the Controller in case the latter is obliged to execute a data privacy impact assessment. The Processor is entitled to invoice the Controller for such assistance on a time and material basis at the then current applicable prices.

4.10 Audits and inspections

The Processor shall:

- permit the Controller, at its own expense, to reasonably inspect and audit the Processor's data Processing activities under this agreement and comply with all reasonable requests or instructions by the Controller to enable the Controller to verify and/or procure that the Processor is in full compliance with its obligations under this agreement; the Controller may request such audit:
- once every twelve (12) months;
- where required by a competent authority under the Personal Data Processing Legislation;
- in case of a Personal Data breach;

when applying its right to audit, the Controller shall comply with its obligations in this regard as provided for under article 5 of this agreement;

- immediately inform the Controller if, in its opinion, a request or an instruction infringes the Personal Data Processing Legislation or other Union or Member State data protection provisions.

Assistance by the Processor will be provided upon agreement between the Parties on the scope, timing and durations and after approval by the Controller of the costs that such assistance will imply for the Processor.

The Controller shall not be entitled to claim compensation for audit expenses incurred by him.

5. Obligations of the Controller

The Controller shall:

- be solely responsible for the lawfulness of the Processing of the Personal Data;
- take reasonable steps to keep the Processed Personal Data up to date in order to ensure that they are accurate and complete with regard to the purpose for which they are Processed;
- duly inform the Data subjects of the Processing;
- comply and continue to comply with the Personal Data Protection Legislation, notably as regards his Processing activities under this agreement and the Main contract, and any other laws and regulations that apply to the Controller; where such laws and regulations, specific to the Controller, his industry, his country of establishment or in which he operates, etc., may have an impact on the Processing of the Processor the Controller shall inform the Processor of such legislation, provide cooperation to the Processor, in order for the latter to make the Processing comply with such laws and regulations and to compensate the Processor if this requires additional services or investments or modification to the Processing or to the services provide under the Main contract;
- inform the Processor without undue delay in case the Processing activities no longer comply with the Personal Data Protection Legislation or in case of any other problem that might have an impact on the Processor;
- instruct the Processor to Process the Personal Data only on his behalf and in accordance with the provisions of the Personal Data Protection Legislation;
- in case he wants to audit the Processor as provided for in article 4.10 of this agreement:
- inform the Processor by prior written notice of thirty (30) calendar days;
- observe all of the Processor's security policies, procedures and measures in place at the time of such audit and, in case the audit takes place at the Processor's premises, conduct such audit:
- strictly within the limits of the policies, procedures and measures regarding access to and use of Processor's facilities taken into account the regulatory status of this latter;
- in the presence of the Processor's staff members, advisors or contractors designated by the Processor for this purpose;
- in a short period of time, to be defined by the Parties, in order not to interrupt the Processor's business and to disturb it the least as possible;
- keep all information relating to Processor (such as, but not limited to the Processor's products and services, operations, customers, members, prospects, know-how, design rights, trade secrets, market information and/or business affairs, etc.) obtained during an audit confidential ("Confidential Information"), unless if it concerns public information;
- not use the Confidential Information for any purpose other than to carry out the audit;
- not disclose Confidential Information to any third party save to its employees, officers and agents to the extent necessary in the framework of such audit and provided that the Controller ensures that such employees, officers and agents are aware of and comply with the confidentiality terms of this article;
- not copy, in whatever way or form, Confidential Information, unless such information is necessary for the audit and return, delete and destroy in primary and backup all Confidential Information after termination of the audit
- notify the Processor immediately and provide relevant details if any non-compliance is discovered during an audit.

6. Liability

The Parties' liability under this agreement is governed by the concerned article(s) of the Main contract, except that the Processor shall indemnify the damage that a Data subject suffers if such damage is caused by Processing activities for which the Processor:

- did not comply with directly applicable obligations for data processors under the Personal Data Protection Legislation;
- departed from the instructions of the Controller and acted on its own decisions.

Where one of the Parties has paid damages to Data subjects that are partly or fully attributable to the other Party, the Party that paid such damages is entitled to claim back the (relevant part of the) damages from the other Party.

7. Term and termination of this agreement

This agreement comes into effect at the same data as the Main contract.

It will automatically terminate upon termination of the Main contract, except for the articles 4.2, 4.4, 4.7 and 4.10 which shall survive the termination of this agreement and shall continue in full force and effect until all Personal Data and existing copies are, at the Controller's choice, returned or deleted. Notwithstanding the above, it is understood that the Processor may be required by Union or Member State law to store the Personal Data.

Termination of this agreement for whatever reason shall not affect the accrued rights or obligations of either Party arising out of this agreement and all provisions which are expressed to survive this agreement (or impliedly do so) shall remain in full force and effect.

8. Severability

If one or more provisions of this agreement are deemed to be invalid or ruled to be invalid in application of a statute or regulation or following a final decision of a competent court, the Parties shall use their best effort to replace it by a valid provision that would have similar effect between the Parties.

In such case the other provisions of this agreement shall remain in full force and effect.

9. Waiver

No failure or delay by any Party in exercising any right or remedy provided by law under or pursuant to this agreement shall impair such right or remedy or operate or be construed as a waiver or variation of it or preclude its exercise at any subsequent time and no single or partial exercise of any such right or remedy shall preclude any other or further exercise of it or the exercise of any other right or remedy.

10. Assignment

This agreement shall not be transferred or assigned by either Party except with the prior written consent of the other.

11. Amendment

No amendment to this agreement shall be valid unless it is in writing and signed by the Parties to it.

12. Governing law, exclusive jurisdiction and domicile

This agreement shall be governed by Dutch law.

In the event of a dispute, the Parties shall seek an amicable settlement to their conflict. In such case, the Parties will meet in order to find a mutual and acceptable solution to such dispute.

Should such amicable settlement not be reached, the dispute shall be submitted to the competent courts of Alkmaar.

Signed on datein place, in two original copies, both Parties acknowledging that they have received their copy.

Company name Controller	**iBabs B.V.**
Name signatory(-ies) title/capacity	M. Lammers, Managing Director

Schedule A

1. Information about the Processing (art. 4 of the data processing agreement)

Nature and purpose of the Processing:	
types of Personal Data Processed:	
Categories of Data subjects:	
Contactperson processor	**M. Lammers, privacy@ibabs.com, +31 229 275850**

Schedule B

1. Technical and organizational security measures (art. 4.2 of the agreement) The

Processor implements the following security measures:

- access to Personal Data is limited to those persons that need to have access to do their job ("authorised persons");
- acces to Personal Data is limited to those data that the authorised persons need to do their job;
- access to the Personal Data is denied to persons that are not or no longer authorised to access them;
- authorisations to access and process the Personal Data are only provided to reliable persons and are regularly verified and updated (e.g. withdrawal of authorisations of ex-personnel, modifications to the scope of access, etc.);
- it has appropriate security audit arrangements in place (e.g. in order to audit who has access to the system, logging of such access, etc.);
- personnel is informed and aware of the security policy and of common methods that can be used to compromise the security policy and measures (e.g. hacker using the telephone to pass a systems maintenance engineer or pretending to be a new employee);
- all computers are password protected against access and that passwords are changed regularly;
- Personal Data are protected against the risk of intrusion, loss, damage, alteration, unauthorised disclosure or acces and destruction by using, amongst others, a secured network, a firewall, a secure backup system, DRP, etc.; - computers have anti-virus software installed and that this software is updated from time to time;]
- pseudonomysation of Personal Data
- encryption of Personal Data
- the Processor is ISO 27001 and ISO9001 certified
- the prevention of unauthorized persons from gaining access to systems Processing Personal Data (physical access control)
- the prevention of systems Processing Personal Data from being used without authorization (logical access control)
- ensuring that persons entitled to use a system Processing Personal Data gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing, Personal Data cannot be read, copied, modified or deleted without authorization (data access control)
- ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control)
- ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from systems Processing Personal Data (entry control)
- ensuring that Personal Data Processed are Processed solely in accordance with the instructions (control of instructions)
- ensuring that Personal Data are protected against accidental destruction or loss (availability control)
- ensuring that Personal Data collected for different purposes can be processed separately (separation control)

Schedule C

List of sub-processors at the date of execution of the data processing agreement

- CYSO hosting BV