MITEK SYSTEMS B.V.
DATA PROCESSING AGREEMENT

THE UNDERSIGNED

1. **FELYX SHARING BV** a company incorporated under the laws of the Netherlands and registered at the Chamber of Commerce under registration number 68094434, with its registered offices at Pilotenstraat 37, 1059CH, Amsterdam, The Netherlands, duly represented by its CEO, 10.2.e (hereinafter, "**Controller**"),

   and

2. **MITEK SYSTEMS B.V.,** a company organized under the laws of The Netherlands, and registered at the Chamber of Commerce under registration number 34242857, with its offices at Radarweg 60, 1043 NT in Amsterdam, duly represented in this matter by its VP & MD, 10.2.e 10.2.e including its affiliates in the EU and its parent company in the United States (hereinafter called **"Processor"**);

Controller and Processor are jointly referred to herein as: **"the Parties"**

CONSIDERING THAT:

- The Controller will have personal data processed by the Processor, which processing is part of the performance of the services (hereinafter called the **"Services"**), which Services have been described in the Service Agreement, as may be amended from time to time, between the Controller and the Processor dated September 22, 2017 (hereinafter called the **"Agreement"**);

- The Processor will processes personal data in the context of the performance of the Agreement only as a "processor" on behalf of and pursuant to the Controller's instructions within the meaning of 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 ("General Data Protection Regulation" or **"GDPR"**), and Controller, either alone or jointly with others, determines the purposes and means of "processing of personal data" and instructs Processor on the processing of personal data and is be the "controller" within the meaning of the GDPR;

- Controller and Processor, also in light of the relevant Articles of the GDPR, wish to formalise the terms and conditions that will be applicable to the processing of personal data by Processor on behalf of Controller, in this agreement (hereinafter called the **"Data Processing Agreement"**);

AGREE AS FOLLOWS:

1. **Definitions.**
   In this Data Processing Agreement, terms such as '**processing**', '**personal data**', '**data subject**', '**data breach**', '**(data) controller**' and '**(data) processor**' will have the meaning

described in the GDPR, unless explicitly defined differently. In addition, the following term will have the following meaning:

"Applicable Privacy Legislation": Any legislation that applies to the processing of personal data, such as, but not limited to **GDPR.**

2. **Subject of the Agreement.**

2.1 The Processor undertakes to process personal data on the terms and conditions of this Data Processing Agreement and only in accordance with the written instructions of the Controller and only and to the extent and in such manner as is necessary for the provision of the Services as described in the Agreement. The Processor shall process the personal data properly, with due care and in accordance with the Applicable Privacy Legislation relating to the processing of personal data.

2.2 The control of the personal data remains with Controller and Controller will at all times remain the data controller for the purpose of the Agreement and the Data Processing Agreement. Controller is responsible for compliance with its obligations as data controller under the Applicable Privacy Legislation, in particular for justification of any transmission of personal data to Processor (including providing any required notices, information and obtaining any required consents), and for its decisions and actions concerning the Processing and use of the personal data.

2.3 The Processor will promptly inform the Controller of any impossibility on the part of the Processor to meet the Controller's written instructions.

3. **Controller and Processor's Obligations.**

3.1 The Processor shall only process the personal data on and in accordance with the instructions of the Controller. The Processor may not process the personal data for its own benefit, for the benefit of third parties, and/or for its own purposes or advertising purposes or other purposes.

3.2 The Processor shall not retain personal data made available to it in the context of the Agreement any longer than is necessary (i) for the performance of this Agreement; or (ii) to comply with any of its statutory obligations.

3.3 The Processor will promptly inform the Controller of any claim from any data subject or third party in connection with any violation of the Applicable Privacy Legislation, and of all other communication with or from any data subject and/or any third party, or a third party engaged on his or their behalf concerning the personal data.

3.4 Controller is responsible for compliance with all Applicable Privacy Legislation.

4. **Processing in European Economic Area ("EEA").**

4.1 The Processor guarantees that it will not process any personal data outside the EEA or export personal data out of the EEA, except to countries and/or organizations that the European Commission deemed adequate to enable data transfers under EU law, such as the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks ("**Privacy Shield**"). The Processor is aware of the fact that the Processing of personal data in and/or the export of personal data to any country outside the EEA (or a country without an adequate level of protection according to the Applicable Privacy Legislation) may violate the Applicable Privacy Legislation and other relevant privacy regulations, and that this is therefore prohibited without the Controller's prior written consent.

5. **Security - Technical and Organisational Measures.**

5.1 The Processor shall implement appropriate technical and organisational measures to secure personal data against loss or any form of unlawful processing. Taking into account the state of the art and the costs of their implementation, these measures guarantee an appropriate security level given the risks associated with Processing and the nature of the personal data to be protected. These measures also focus on preventing unnecessary collection and further Processing. The Processor shall record the measures in writing and shall ensure that the security as referred to in this Section meets with the security requirements under the GDPR. In Annex C to this Data Processing Agreement the implemented technical and organisational (security) measures are described in detail.

5.2 Controller and Processor agree that the implemented security measures (Annex C) currently meet the security requirements under the GDPR. However, the Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. Processor will therefore evaluate the measures, as implemented in accordance with this Section of the Data Processing Agreement, on an on-going basis and will update, supplement and improve these measures in order to maintain compliance with the requirements under the GDPR.

6. **Data Breach / Security Breach.**

6.1 In the event of personal data breach the Processor shall notify the Controller without undue delay, but no later than forty-eight (48) hours after the incident was first discovered. The Processor shall take all measures reasonably necessary to stop and prevent any future breach of personal data. This provision applies to incidents at the Processor and its Sub processors, if any.

6.2 At the Controller's request, the Processor shall cooperate in informing the competent authorities and Data Subject(s).

6.3 The Processor shall make written arrangements with Sub processors about the reporting of incidents to the Processor, which will enable the Processor and the Controller to comply with obligations in the event of an incident as described in Section 6.1. These arrangements must in any event include the obligation that the Sub processor shall notify the Processor immediately, but no later than 48 hours after the first discovery of an incident as described in Section 6.1, and at the Controller's request shall cooperate in informing the competent authorities and the Data Subject(s). In Annex D to this Data Processing Agreement the data breach notification details are listed.

7. **Sub processors.**

7.1 Processor also may engage Sub processors to assist in the provision of the Services. Processor maintains a list of Sub processors that may process the personal data and will attach a copy of that list to this Data Processing Agreement (Annex B).

7.2 All Sub processors are required to abide by substantially the same obligations as Processor under this Data Processing Agreement as applicable to their performance of Services. Controller may request that Processor audit the Sub processor or provide confirmation that such an audit has occurred (or, where available, obtain or assist Controller in obtaining a third-party audit report concerning Sub processor's operations) to ensure compliance with such obligations. Controller also will be entitled, upon written request, to receive copies of the relevant terms of Processor's agreement with Sub processors that may Process personal data, unless the agreement contains confidential information, in which case Processor may provide a redacted version of the agreement.

7.3 Processor remains responsible at all times for compliance with the terms of the Agreement and this Data Processing Agreement by Processor, its affiliates and sub processors.

7.4 Controller consents to Processor's use of the listed Sub processors in the performance of the Services in accordance with the terms of this Data Processing Agreement. Processor undertakes that these Sub processors are not allowed to engage with other subcontractors, without the prior written approval of Processor (and so Processor requires Controller's prior written approval).

8. **Audit Rights.**

8.1 Controller may audit Processor's compliance with the terms of the Agreement and this Data Processing Agreement up to once per year. If a third party is to conduct the audit, the third party must be mutually agreed to by Controller and Processor and must execute a written confidentiality agreement acceptable to Processor before conducting the audit.

8.2 To request an audit, Controller must submit a detailed audit plan at least two weeks in advance of the proposed audit date to Processor describing the proposed scope, duration, and start date of the audit. Processor will review the audit plan and provide Controller with any concerns or questions. Processor will work cooperatively with Controller to agree on a final audit plan. If the requested audit scope is addressed in an audit report performed by a qualified third-party auditor within the prior twelve months and Processor confirms there are no known material changes in the controls audited, Controller agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

8.3 The audit must be conducted during regular business hours at the applicable facility, subject to Processor policies, and may not unreasonably interfere with Processor business activities.

8.4 Controller will provide Processor any audit reports generated in connection with any audit under this Section, unless prohibited by law. Controller may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of the Agreement and this Data Processing Agreement. The audit reports are confidential information of the parties under the terms of the Agreement and Data Processing Agreement.

8.5 Any audits are at the Controller's expense. Any request for Processor to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those requires for the provision of the Services as described in the Agreement. Processor will seek the Controller's written approval to pay any related fees before performing such audit assistance.

9. **Liability.**

9.1 Processor's liability is limited by the relevant Sections of the Agreement. In no event shall either party be liable to the other party for any indirect, punitive, special, incidental, exemplar or consequential or other indirect damages (including loss of profits, loss of revenue, or other loss of economic advantage) under any cause of action arising out of or relating to this Data Processing Agreement.

10. **Informing Data Subjects.**

10.1 The Processor shall assist where needed, so that the Controller can comply with its legal obligations in the event that a data subject exercises its rights under the Applicable Privacy Legislation concerning the processing of personal data.

10.2 If a data subject, in relation to the execution of its rights under the GDPR, contacts the Processor directly, the Processor shall not initially respond (substantively) - unless expressly instructed otherwise by the Controller - but shall immediately report this to the Controller, with a request for further instructions.

11. **Investigation Request.**

11.1 If the Processor receives a request or order from the Dutch or foreign supervisory authority, government agency or investigation, prosecution or national security agency to provide (access to) personal data, the Processor shall immediately notify the Controller. When handling the request or order, the Processor shall observe all of the Controller's instructions (including the instruction to leave the handling of the request or order in full or in part to the Controller) and provide all reasonably required cooperation to the Controller.

12. **Confidentiality.**

12.1 In the event that the confidentiality of data is not provided for in the Agreement or any other existing contractual arrangement between the Parties, the Parties shall keep confidential all (personal) data and other information, the confidential nature of which they are aware of or can reasonably suspect, and that have come to their attention or to which they obtained access in the context of the performance of the Agreement or the Data Processing Agreement, and shall refrain from disclosing these internally or externally and/or providing these to third parties, except in so far as:

a. disclosure and/or provision of said (personal) data and other information is necessary in the context of the performance of the Agreement or the Data Processing Agreement;

b. any mandatory statutory provision or court decision requires the Parties to disclose and/or provide said (personal) data or other information, in which case the Parties shall first notify the other party unless prohibited by law or court order;

c. disclosure and/or provision of said (personal) data and other information takes place with the prior written consent of the other party; or

d. it concerns information that has already been legitimately disclosed in a manner other than through the acts or omissions of one of the Parties.

12.2 Processor will inform all its employees, agents and permitted subcontractors engaged in processing personal data of the confidential nature of such personal data and information. Further, Processor shall maintain appropriate written agreements with its employees, agents, permitted subcontractors or other (third) parties with access to such personal information to enable it to comply with the terms of this Data Processing Agreement.

13. **Term and Termination.**

13.1 This Data Processing Agreement will come into effect as of the signing date thereof and remains in force for as long as the Agreement remains in force, unless terminated earlier in accordance with this Section 13.

13.2 If a party has not remedied any material breach of this Data Processing Agreement notified to it by the other party within forty-five (45) days after receipt of such notice, the other party is entitled to terminate this Data Processing Agreement by notice to the failing party without prejudice to any other rights accruing under this Data Processing Agreement or in law.

13.3 This Data Processing Agreement may also be terminated by either Party in writing with immediate effect in the event that the other Party:

- Files for voluntary bankruptcy or submits an application for bankruptcy;
- is the subject of an involuntary bankruptcy petition that is not discharged within 60 days

- has a receiver appointed for all or a portion of its assets
- has its assets assigned for the benefit of its creditors; or
- discontinues its business or ceases to operate as a going concern.

14. **Access to Personal Data.**

14.1 The Processor will only disclose the data provided by the Controller to those employees and third parties engaged by the Processor on a need to know basis within the framework of this Data Processing Agreement.

14.2 Upon Controller's first written request or upon termination of the Data Processing Agreement, the Processor will promptly return or destroy all personal data provided by the Controller.

15. **Storage of data**

15.1 Pursuant to Article 5e of GDPR the Controller is committed to not store personal data longer than is necessary for the purposes for which the personal data are processed (or as required by law) and to handle all personal data in strict compliance with GDPR.

16. **Indemnification.**

16.1 The Controller shall defend, indemnify and hold the Processor harmless, and will support Processor where necessary, against any third party claim arising as a result of Controller's breach of the terms of this Data Processing Agreement or as a result that Controller not complying with any applicable law, Applicable Privacy Legislation or GDPR.

17. **Miscellaneous.**

17.1 Amendments and additions to this Data Processing Agreement and the relevant Annexes thereto will only be valid and binding if these amendments and additions are agreed in writing and have been signed by both Parties.

17.2 This Data Processing Agreement is governed by the laws of the Netherlands. Any disputes arising out or in connection with this Data Processing Agreement will be brought exclusively before the competent courts of Amsterdam, The Netherlands.

[signature page follows]

Thus agreed and signed in duplicate:

On behalf of the Controller:

10.2.e

FELYX SHARING B.V.

Name: 10.2.e

Title: CPO

Date: January 17, 2020

Place: Amsterdam

On behalf of the Processor:

10.2.e

MITEK SYSTEMS B.V.

Name: 10.2.e

Title: VP & MD

Date: January 17, 2020

Place: Amsterdam

ANNEX A – SPECIFICATION OF PROCESSING PERSONAL DATA

1. PURPOSE OF THE PROCESSING:

Processing personal data is directly related to the performance of the Services described in the Agreement. In short, these Services include:

Provision of identity verification results

2. DATA SUBJECTS:

Consumer Customers of Controller

3. PERSONAL DATA CATEGORIES:

The Processor will process the following personal data (categories) for the Controller:

ID documents, such as Passports, Identity Cards, Drivers Licenses and/or Residence Permits containing: Name(s), Dates of Birth, Place of Birth, Gender, Nationality, Date of Issue, Date of Expiry, Document Number, national identification number, photo, signature, etc. (if applicable in ID submitted).

The following special categories of personal data can be processed for the Controller *(if applicable in ID submitted)*: ***photo (only if handled automated by a biometric solution)***

4. ACCESS TO PERSONAL DATA

Personnel involved in the processing of the personal data to provide the identity verification results.

5. STORAGE & DATA RETENTION

Per the Agreement

ANNEX B - LIST OF SUBPROCESSORS

The Processor engages the following sub processors in the performance of the Agreement:

1. Amazon Web Services – Hosting Provider (with no access to the Controller's consumer data).

2. LeaseWeb Netherlands BV – Hosting Provider (with no access to the Controller's consumer data).

ANNEX C – SPECIFICATION TECHNICAL AND ORGANISATIONAL (SECURITY) MEASURES

Attached is the ISO27001 certificate & where applicable a Statement of Applicability specifying the implemented controls.

ANNEX D – MITEK DATA BREACH NOTIFICATION REPORT

	CONTACT CONTROLLER	CONTACT PROCESSOR
Company	Felyx Sharing B.V.	Mitek Systems B.V.
Name	10.2.e	10.2.e
Title	CEO	VP & MD
E-mail address	10.2.e @felyx.nl	10.2.e @miteksystems.com
Phone number	10.2.e	10.2.e
Emergency phone number	10.2.e	10.2.e

Report details:

Where applicable the following incident details will be reported:

- Incident Title
- Date of discovery/notification
- High level summary of incident (summarized in bulleted format)
- People/roles involved: e.g. contractors, government, employees, etc.
- Type of PII (presumably) compromised
- Ownership of the PII
- Estimation of number of individuals impacted
- Description of current status / situation
- Remedial steps taken (immediate & where possible steps/actions planned)