Annex 1

Data Processing Agreement

between

Customer

(hereinafter "**Controller**")

and

KYC Spider AG

Gubelstrasse 11

6300 Zug

(hereinafter "**Processor**")

regarding

Preamble

This Annex details the parties' obligations on the protection of personal data, associated with the processing of personal data on behalf of Controller as a data controller, and described in detail in the agreement. Its regulations shall apply to any and all activities associated with the Agreement, in whose scope Processor's employees or agents process Controller's personal data (hereinafter, "Data") on behalf of Controller as a controller (hereinafter, "Contract Processing").

I. Scope, duration and specification of contract processing of Data

1. The scope and duration and the detailed stipulations on the type and purpose of Contract Processing shall be governed by the Agreement. Specifically, Contract Processing shall include, but not be limited to, the following:

   a) Purpose of processing

   The online services, specifically the Toolbox (SaaS Platform), are an instrument for checking an entity on relevant information regarding money laundering. For this purpose, KYC provides the KYC Records. With the access to / search in the online services of KYC Spider, the extended identification obligations of the financial intermediary according to the Federal Act on Combating Money Laundering and Terrorist Financing (AMLA as of 1st January 2016) are fulfilled. The financial intermediary detects client relationships with sanctioned persons/organisations (i.e. data pursuant to Art. 22a AMLA) and PEP background (i.e. qualification characteristics pursuant to art. 2a para. 2 AMLA). In addition, KYC Records shows references to further detectable and clarification-relevant in-formation. Finally, KYC Records enables a traceable documentation of the corresponding clarification.

   b) Description and scope of data processing

   Data of Entity to be checked (Data of Customers of Controller) will be processed and stored. In the course of the usage of the individual Tools, the following data, among others, will be collected:

      i) Organization

      ii) Surname and Name

      iii) Date of birth

      iv) Country of origin

      v) Country of residence

      vi) E-Mail-Address

      vii) Other data requested in the form or via the chatbot and entered by the Controller/the person to be checked

The **data** of the entity to be checked **will be deleted after four weeks**. The Controller is responsible to download all documents and data and store them for possible audit purposes.

However, it is possible to store all documents and data with the contractor after the order has been placed, which is regulated by the contract between the Controller and the contractor. The Controller explicitly consents to the contract by signing and ordering the "Document Store" service, OR/AND informs the Contractor.

2. For further information please see the Platform Policy of the Processor.

   Platform Dataprivacy Policy

3. Except where this Annex stipulates obligations beyond the term of the Agreement, the term of this Annex shall be the term of the Agreement.

II. Scope of application and responsibilities

1. Processor shall process Data on behalf of Controller. Such Contract Processing shall include all activities detailed in the Agreement and its statement of work. Within the scope of this annex, Controller shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Processor and the lawfulness of having Data processed on behalf of Controller. Controller shall be the “controller” in accordance with Article 4 no. 7 of the GDPR.

2. Controller’s individual instructions on Contract Processing shall, initially, be as detailed in the Agreement. Controller shall, subsequently, be entitled to, in writing or in a machine-readable format (in text form), modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Processor. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the statement of work. Controller shall, without undue delay, confirm in writing or in text form any instruction issued orally.

III. Processor’s obligations

1. Except where expressly permitted by Article 28 (3)(a) of the GDPR, Processor shall process data subjects’ Data only within the scope of the statement of work and the instructions issued by Controller. Where Processor believes that an instruction would be in breach of applicable law, Processor shall notify Controller of such belief without undue delay. Processor shall be entitled to suspending performance on such instruction until Controller confirms or modifies such instruction.

2. Processor shall, within Processor’s scope of responsibility, organise its internal organisation so it satisfies the specific requirements of data protection. Processor shall implement technical and organisational measures to ensure the adequate protection of Controller’s Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. Processor shall implement technical and organisational measures and safeguards

that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. Controller is familiar with these technical and organisational measures, and it shall be Controller's responsibility that such measures ensure a level of security appropriate to the risk. (Appendix 1)

Processor reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.

3. Processor shall support Controller, as far as agreed upon by the parties, and where technical possible for Processor, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR.

4. Processor warrants that all employees involved in Contract Processing of Controller's Data and other such persons as may be involved in Contract Processing within Processor's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Processor warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.

5. Processor shall notify Controller, without undue delay, if Processor becomes aware of breaches of the protection of personal data within Processor's scope of responsibility.

   Processor shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Processor shall coordinate such efforts with Controller without undue delay.

6. Processor shall notify to Controller the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

7. Processor warrants that Processor fulfils its obligations under Article 32 (1)(d) of the GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

8. Processor shall correct or completely delete Data if instructed by Controller and where covered by the scope of the instructions permissible. Where a complete correction or deletion, compliant with data protection requirements, or a corresponding restriction of processing is impossible, Processor shall, based on Controller's instructions, and unless agreed upon differently in the Agreement, destroy, in compliance with data protection requirements, all carrier media and other material or return the same to Controller.

   In specific cases designated by Controller, such Data shall be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement.

9. Processor shall, upon termination of Contract Processing and upon Controller's instruction, return all Data, carrier media and other materials to Controller or delete the same.

Controller shall bear any extra cost caused by deviating requirements in returning or deleting data.

10. Where a data subject asserts any claims against Controller in accordance with Article 82 of the GDPR, Processor shall support Controller in defending against such claims, where possible.

IV. Controller's obligations

1. Controller shall notify Processor, without undue delay, and comprehensively, of any defect or irregularity regarding provisions on data protection detected by Controller in the results of Processor's work.

2. Section 3 para. 10 above shall apply, mutatis mutandis, to claims asserted by data subjects against Processor in accordance with Article 82 of the GDPR.

3. Controller shall notify to Processor the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

V. Enquiries by data subjects

Where a data subject asserts claims for rectification, erasure or access against Processor, and where Processor may correlate the data subject to Controller, based on the information provided by the data subject, Processor shall refer such data subject to Controller. Processor shall forward the data subject's claim to Controller without undue delay. Processor shall support Controller, where possible, and based upon Controller's instruction to the extent agreed upon. Processor shall not be liable in cases where Controller fails to respond to the data subject's request in total, correctly, or in a timely manner.

VI. Options for documentation

1. Processor shall document and prove to Controller Processor's compliance with the obligations agreed upon in this exhibit by appropriate measures.

   Where specific types of documentation and proof can be identified, with regards to compliance with the obligations agreed upon, Processor may make available to Controller the following:

   Conducting an own self-audit.

2. Where, in individual cases, audits and inspections by Controller or an auditor appointed by Controller are necessary, such audits and inspections will be conducted during regular business hours, and without interfering with Processor's operations, upon prior notice, and observing an appropriate notice period. Processor may also determine that such audits and inspections are subject to prior notice, the observation of an appropriate notice period, and the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organisational measures and safeguards implemented. Processor shall be entitled to rejecting auditors which are competitors of Processor.

Controller hereby consents to the appointment of an independent external auditor by Processor, given that Processor provides a copy of the audit report to Controller.

Processor shall be entitled to requesting a remuneration for Processor's support in conducting inspections. The cost of an inspection is generally limited to one day per calendar year for the Processor; this can be extended as required if the Controller remunerates the cost accordingly.

3. Where a data protection supervisory authority or another supervisory authority with statutory competence for Controller conducts an inspection, para. 2 above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

VII. Subcontractors (further processors)

1. Processor shall use subcontractors as further processors on behalf of Controller which are accepted with the use of the KYC Spider Services. Information on the respective subcontractors can be found in the Platform Data Privacy Policy:

   Platform Dataprivacy Policy

2. A subcontractor relationship shall be commissioning further processor or subcontractors with the performance agreed upon in the Agreement, in whole or in part. Processor shall conclude, with such subcontractors, the contractual instruments necessary to ensure an appropriate level of data protection and information security.

   Controller hereby consents to Processor's use of subcontractors. When engaging or replacing subcontractors, the Contractor shall inform the Customer by adapting and posting the new Platform Data Privacy Policy on the KYC Spider website.

   Controller shall be entitled to contradict any change notified by Processor within 30 days and for a legally relevant reason. Where Processor fails to contradict such change within such period, Controller shall be deemed to have consented to such change. Where a materially important reason for such contradiction exists and failing an amicable resolution of this matter by the parties, Controller shall be entitled to terminating the Agreement (subscription fees/costs are due in any case).

3. Where Processor commissions subcontractors, Processor shall be responsible for ensuring that Processor's obligations on data protection resulting from the Agreement and this exhibit are valid and binding upon subcontractor.

VIII. Obligations to inform, mandatory written form, choice of law

1. Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Processor's control, Processor shall notify Controller of such action without undue delay. Processor shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in Controller's sole property and area of

responsibility, that data is at Controller's sole disposition, and that Controller is the responsible body in the sense of the GDPR.

2. No modification of this Annex and/or any of its components – including, but not limited to, Processor's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this annex. The foregoing shall also apply to any waiver or modification of this mandatory written form.

3. In case of any conflict, the data protection regulations of this annex shall take precedence over the regulations of the Agreement. Where individual regulations of this annex are invalid or unenforceable, the validity and enforceability of the other regulations of this annex shall not be affected.

4. This annex is subject to the laws of Switzerland.

IX. Liability and damages

The regulations on the parties' liability contained in the Agreement shall be valid also for the purposes of Contract Processing, unless expressly agreed upon otherwise.

Appendix - Technical and Organisational Measures

Appendix 1 - Technical and Organisational Measures

1. Confidentiality (Article 32 Paragraph 1 lit. b GDPR)

- Physical Access Control
  No unauthorised access to Data Processing Facilities (chip cards, keys)
- Access Control
  No unauthorised use of the Data Processing Systems (secure passwords)
- Internal Access Control
  No unauthorised Reading, Copying, Changes or Deletions of Data within the system (rights authorisation concept, need-based rights of access)

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- Data Transfer Control
  No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport (Encryption [https])

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- Availability Control
  Prevention of accidental or wilful destruction or loss (Continuous control with monitoring system (currently Nagios));

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data Protection Management