Schedule 2

Data processing agreement

*Capitalised words and meanings not defined in this data processing agreement (this "**DPA**") will have the meaning ascribed to such term in KnownID's general terms and conditions (the "**Terms and Conditions**").*

1. Introduction

1.1. KnownID AB, Reg. No. 559432-3924 ("**KnownID**") provides a platform for (a) sharing and managing KYC information and documentation and (b) e-learning (the "**Platform**"), where companies, organisations, and others who has created a business account (a "**Business User**") is given the right to use certain digital services and features (the "**Services**").

1.2. In order to provide the Services to the Business User, KnownID will process personal data and other information on behalf of the Business User. For that reason, the Parties have agreed to regulate the conditions for KnownID's processing of, and access to, personal data on behalf of the Business User in this DPA.

1.3. This DPA consists of this document and the attached instruction (the "**Instruction**"). In the event of any contradiction between this document and the Instruction, this document prevails, unless otherwise specified or unless circumstances clearly dictate otherwise.

1.4. For the purpose of this DPA, the terms "controller", "processor", "data subject", "personal data", "process", and "personal data breach" have the same meaning as set out in the EU General Data Protection Regulation (the "**GDPR**").

2. Generally regarding the processing

2.1. The Business User is the controller of the personal data processed in connection with the Business User's use of the Services. KnownID is to be considered a processor to the Business User for the processing of personal data carried out by KnownID on behalf of the Business User.

2.2. The Business User authorises KnownID to transfer any personal data to third parties as necessary to fulfil the Services, fulfil the purpose of this DPA, including the Instruction, and/or to fulfil a legal obligation. This includes, but is not limited to, transferring the personal data to suppliers, partners and authorities.

2.3. KnownID may only process personal data based on the Business User's documented instructions as set out herein and according to applicable law. In the event KnownID would find that instructions necessary to carry out the assignment is missing or that instructions given by the Business User are contrary to applicable law, KnownID must notify the Business User without undue delay. In addition, KnownID is not obliged to follow instructions which, in the opinion of KnownID, are contrary to applicable law. In such event, KnownID may take any actions that it deems are necessary to comply with applicable law.

2.4. KnownID may process certain relevant information for its own purposes in its role as data controller (such as e.g. invoicing information). KnownID must provide information about such processing in its privacy notice as applicable from time to time.

3. Agreement term and actions upon termination

3.1. This DPA is valid as from execution and remains in force for as long as KnownID or any sub-processor retained by KnownID processes personal data on behalf of the Business User within the scope of the undertakings arising from this DPA.

3.2. KnownID undertakes to erase all personal data related to the Business User sixty (60) days after the provision of processing services has ended (ie upon closure of the Business User's Business Account (as defined in the Terms and Conditions)), unless storage of the personal

data is required by applicable law or if KnownID has a legal basis to process relevant personal data.

4. Confidentiality

KnownID must ensure that its employees and all other persons for whom KnownID is responsible and who are authorised to process personal data covered by this DPA undertake to observe confidentiality or are subject to a relevant and appropriate statutory duty of confidentiality.

5. Security

5.1. KnownID must take all necessary security measures required in accordance with Article 32 of the GDPR and this DPA.

5.2. In assessing the appropriate level of security in accordance with the clause above, particular account must be taken of the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss or alteration, or from unauthorised disclosure of, or access to, the personal data transmitted, stored, or otherwise processed.

5.3. Taking into account the type of the processing and the information in possession of KnownID, KnownID undertakes to assist the Business User in ensuring that the Business User's obligations regarding security can be fulfilled in the manner which follows from Article 32 of the GDPR.

6. Personal data breach

6.1. KnownID must notify the Business User without undue delay after becoming aware of a personal data breach related to the Business User.

6.2. A notification according to section 6.1 must contain information regarding:

(i) the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(ii) the name and contact details of a contact person where more information can be obtained,

(iii) the likely consequences of the personal data breach, and

(iv) the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its potential adverse effects.

6.3. Where, and in so far as, it is not possible to provide the information according to section 6.2 at the same time, the information may be provided in phases without undue further delay.

6.4. Taking into account the type of processing and the information available to KnownID, KnownID undertakes to assist the Business User to a reasonable extent in ensuring that the obligations in connection with any personal data breach can be fulfilled in the manner which follows from Articles 33–34 of the GDPR as well as the performance of a data protection impact assessment and/or prior consultation with a supervisory authority in accordance with Articles 35 and 36 of the GDPR.

7. Sub-processors

7.1. The Business User has approved the sub-processors retained by KnownID at the date hereof and which are set out in the Instruction.

7.2. KnownID undertakes to inform the Business User of any plan to retain a new sub-processor and/or replace existing sub-processors with minimum thirty (30) days prior notice unless a

shorter notice is agreed by the Business User. If the Business User does not object during the notice period, the Business User is deemed to have accepted the prospective sub-processor(s). If the Business User would object to a prospective sub-processor(s), the Parties agree to cooperate to find an appropriate solution. The Business User has the right to immediately terminate this DPA (and thereby close its Business Account), if an appropriate solution cannot be found.

7.3. KnownID must ensure that each sub-processor enters into a written data processing agreement (no less protective than as set out herein) before such sub-processor commences work that has a connection to the Business User. KnownID remains responsible to the Business User for the sub-processor's fulfilment of its obligations under this DPA.

7.4. KnownID may transfer, store, transmit, or otherwise process personal data on behalf of the Business User outside the EU/EEA, provided KnownID, before transfer to a third country commences, complies with the requirements and measures that follow from the GDPR or other applicable law with regard to third country transfers. KnownID undertakes, where applicable, to enter into the EU Commission’s Standard Contractual Clauses (SCC) or equivalent transfer mechanism with sub-processors whose operations are outside the EU/EEA.

8. Request for information

8.1. If a data subject or other third-party requests information from KnownID regarding processing of personal data carried out on behalf of the Business User, KnownID must refer such data subject or other third party to the Business User.

8.2. If a public authority requests information from KnownID regarding processing of personal data carried out on behalf of the Business User, KnownID must notify the Business User without undue delay unless prohibited by law and, in consultation with the Business User, agree on an appropriate course of action. KnownID does not have the right to represent the Business User or act on their behalf vis-à-vis the public authority.

8.3. Taking into account the nature of the processing, KnownID must, through appropriate technical and organisational measures, assist the Business User, to the extent possible, so that the Business User can fulfil its obligation to respond to requests regarding exercise of the rights of the data subject in accordance with Chapter III of the GDPR.

9. Right to transparency

9.1. KnownID must provide the Business User with access to all information reasonably required to demonstrate that the obligations which follow from Article 28 of the GDPR have been fulfilled, and to a reasonable extent make possible and contribute to audits, including inspections, conducted by the Business User or by other auditor authorised by the Business User. Unless otherwise agreed in writing, each Party bears its own costs for the audit or inspection according to this clause 9.

9.2. The Business User is responsible for ensuring that personnel and others retained by the Business User to conduct an audit or inspection in accordance with section 9.1 above have entered into a customary confidentiality undertaking that prevents the dissemination of data covered by the audit/inspection.

9.3. The Business User must provide thirty (30) days prior written notice to KnownID prior to an audit or inspection. The audit or inspection must be made in a way which entails the least possible impact on KnownID’s operations. The audit or inspection must also be made in compliance with any security measures provided by KnownID, provided that the measures do not prevent or significantly complicates the audit or inspection.

10. Additions and changes

10.1. KnownID may add and/or change this DPA in a manner decided by KnownID no later than thirty (30) days before such addition or change take effect. If the Business User would object to such change and/or addition during the notice period, and the Business User has:

(i) a Full Business Account or an E-learning Account (as defined in the Terms and Conditions), KnownID may choose to apply the previous DPA for the reminder of the agreement term as set out in the Service Agreement. If KnownID would apply the changed DPA the Business User may terminate this DPA (and thereby close its Full Business Account) at the last day of the notice period.

(ii) a Limited Business Account (as defined in the Terms and Conditions), the Business User may terminate this DPA and close its Limited Business Account at the last day of the notice period.

10.2. In addition, KnownID may with immediate effect and without prior notice make such changes to this DPA that (i) are required by law, regulation or decision by applicable authorities (unless the change is less favourable to the Business User in which case KnownID will provide a notice or a notification within the Platform); and/or (ii) neither reduce the Business User's rights nor increase the Business User's responsibilities.

11. Notices

Any notices and other communications from the Business User to KnownID under this DPA must be made in writing via e-mail, in the Swedish or English language, to privacy@knownid.io. Any notices and other communication from KnownID to the Business User must be made in writing via email to the contact person set out in the Service Agreement, or as specified within the Platform. A notice is deemed to have been received by a Party on the day of delivery. Each Party is responsible for keeping their contact information up to date.

12. Liability

12.1. A Party's liability to compensate for damage/loss that it, or another party for which it is liable, has caused to the other Party in connection with processing of personal data, or in the event of actions in breach of this DPA, is covered by the limitation of liability in clause 9 (Limitation of liability) in the Terms and Conditions.

12.2. Any penalty fees according to Article 83 of the GDPR, or Chapter 6 Section 2 of the Act containing supplementary provisions to the EU General Data Protection Regulation (SFS 2018:218) must be borne by the Party which was imposed such fee by a supervisory authority.

12.3. A Party must inform the other Party immediately if it becomes aware of any impropriety that could lead to damage/loss of the other Party. In such event, the Parties agree to cooperate and work proactively together to prevent and/or minimize such damage/loss.

13. Governing law and jurisdiction

This DPA is governed by the substantive law of Sweden. Any dispute, controversy or claim arising out of or in connection with this DPA, or the breach, termination or invalidity thereof, shall be finally settled by arbitration as set out in the Terms and Conditions.

***

Appendix 1

Instruction to the data processing agreement

Definitions used in this instruction shall have the same meaning as in the DPA, unless the circumstances clearly indicate otherwise.

1. Processing of personal data

Item	Personal data processing
Subject and purpose of KnownID's processing of personal data on behalf of the Business User	Subject and purpose of the processing: ▪ Provide a platform for sharing and managing KYC information and documentation ▪ Provide an e-learning platform
KnownID may process the following categories of personal data on behalf of the Business User	Categories of personal data: ▪ Name ▪ Address ▪ Role ▪ E-mail address ▪ Telephone number ▪ Personal identity number ▪ Place of birth ▪ Date of birth ▪ Nationality ▪ Tax residency ▪ Identity verification data ▪ PEP status ▪ Criminal convictions and offences or related security measures ▪ Other information as provided by the Business User
KnownID may process the following categories of sensitive personal data on behalf of the Business User	Categories of sensitive personal data: ▪ Political opinions (deriving from PEP screening)
KnownID may process personal data relating to criminal convictions and offences or related security measures on behalf of the Business User	Categories of criminal offence data: ▪ Data deriving from sanction screening ▪ Data deriving from adverse media screening
KnownID may process personal data relating to the following categories of data subjects	Categories of data subjects: ▪ The owners, directors, employees and consultants and other key persons of the Business User ▪ The owners, directors, employees and consultants and other key persons of any of the Business User's counterparties

2. Duration of the processing

KnownID will process personal data on behalf of the Business User during the following time period:

Maximum sixty (60) days after the data is either deleted by the Business User or after the Business User's account is closed.

3. Approved sub-processors

The Business User has approved KnownID's use of the following sub-processors:

IT and Infrastructure Services

Service providers involved in hosting, cloud storage, and IT security, such as cloud service providers, data centers, and security monitoring services.

Service provider (sub-processor)	Agreement date	Service description	Geographic processing of data
DigitalOcean	20 June 2023	Cloud services and data storage	Server location: Germany See https://www.digitalocean.com/trust/subprocessors for information on sub-processors
MongoDB	27 July 2023	Cloud services and data storage	Server location: Sweden See https://www.mongodb.com/products/platform/trust/subprocessors for information on sub-processors
Thinkific	6 October 2025	Service supplier for e-learning platform, including cloud services and data storage	Server location: U.S. See https://www.thinkific.com/thinkificsubprocessors/ for information on sub-processors *Transfer to third countries subject to EU standard contractual clauses*

Technology Tooling

Service providers used to automate and manage platform-related tasks, such as email automation for login notifications, system-triggered messages, and other operational workflows.

Service provider (sub-processor)	Agreement date	Service description	Geographic processing of data
Twilio	7 June 2023	Email automation	Server location: USA See https://www.twilio.com/en-us/legal/sub-processors for information on sub-processors *Part of the EU-U.S. Data Privacy Framework. See https://www.dataprivacyframework.gov/list for more information.*

Product Partnerships

External systems or applications integrated into the Platform for additional functionality, such as PEP and sanctions screening providers, and ID verification providers. These service providers are used only where the corresponding product is utilised.

Service provider (sub-processor)	Agreement date	Service description	Geographic processing of data
Criipto	4 Juli 2024	Digital ID verification (eID)	Server location: EU
ComplyAdvantage	15 June 2023	PEP, sanction and adverse media screening	Server location: Ireland See https://complyadvantage.com/sub-processors-list/ for information on sub-processors