DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the Services Agreement signed by you (the "**Client**") when you created your account (the "**Agreement**").

1. **Definitions**. Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement. In the event of any conflict between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Information.

   a. "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100 et. seq., and its implementing regulations.

   b. "**CPA**" means the Colorado Privacy Act of 2021.

   c. "**Data Controller**" (or the "**Controller**") a legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information and gives instructions regarding processing activities to Certn; for the purposes of the Agreement the Client is the Data Controller.

   d. "**Data Processor**" (or the "**Processor**") means the legal entity that processes the Personal Information on behalf of the Data Controller; for the purposes of the Agreement Certn, as defined in the Agreement, is the Data Processor.

   e. "**Data Subject Access Request**" means a form for the Consumer (or the "**Data Subject**" as defined in GDPR) to request access, copy, amendment, dispute, delete or any additional actions to their Personal Information subject to the applicable Data Protection Legislation.

   f. "**FADP**" the Swiss Federal Act on Data Protection.

   g. "**GDPR**" means the European Union's General Data Protection Regulation (EU) 2016/679.

   h. **"LGPD"** General Data Protection Law (Lei Geral de Proteção de Dados).

   i. "**Personal Information**" or "**Personal Data**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable Consumer, which is processed by Certn solely on behalf of the Client, under this DPA and the Agreement.

   j. "**Processing**" (or "**Process**" or "**Processed**") means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

   k. "**Processing Purpose**" the Permissible Purpose, as defined in the Agreement.

   l. "**Standard Contractual Clauses**" ("**SCCs**") means the Standard Contractual Clauses as set out **here** forming part of this with respect to Controller to Processor transfers pursuant to the European Commission's Decision (EU) 2021/914 of 4 June 2021 (as maybe updated by the European Commission from time to time).

   m. "**Sub-processor**" means a Sub-processor engaged, appointed and supervised by Certn who agrees to receive and process Personal Information under the terms of this DPA and solely for the purposes of processing or delivering data, subject to the terms of the Agreement.

   n. **"UK Data Protection Laws"** means all laws relating to data protection, the processing of Personal Information, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

   o. **"UK GDPR"** means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

   p. "**VCDPA**" means the Virginia Consumer Data Protection Act.

2. **Roles**. The Parties acknowledge and agree that with respect to the Processing and transfers of Personal Information subject to the material and territorial scope of GDPR, FADP, LGPD, CPA and the VCDPA : (i) the Client is the Controller of Personal Information; (ii) Certn is the Processor of such Personal Information; and (iii) for the purposes of the CCPA (and to the extent applicable), Client is the "**Business**" and Certn is the "**Service Provider**" (as such terms are defined in the CCPA). As a Consumer Reporting Agency ("**CRA**"), Certn is not considered a data broker and is therefore exempt from the CCPA (see Section 1798.99.80 (d) (1)). The California Civil Code includes exemptions for CRAs (see §1798.145(d)(1) for details).

3. **General**.

   a. Each Party shall comply with all Applicable Laws with respect of its handling of Personal Information and undertakes to use best efforts to assist the other in each Party's compliance with any obligations under Applicable Laws and shall not perform its obligations under this DPA in such a manner as to cause the other Party to breach any of its obligations under Applicable Laws to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

   b. Certn shall process Personal Information only on documented instructions from the Client in accordance with the Processing Purpose, unless required to do so by the Applicable Laws. Subsequent instructions may also be given by the Client throughout the duration of the Processing of Personal Information. Such instructions shall always be documented.

   c. Certn shall immediately inform the Client if Certn believes that the instructions given by the Client (or Controller) infringe Applicable Laws.

4. **Purpose limitation**. Certn shall only process the Personal Information for the Processing Purpose, to the extent, and in such a manner, as is necessary for the performance of the Services. Certn will not process the Personal Information for any other purpose or in a way that does not comply with the Agreement (including this Schedule) or Applicable Laws.

5. **Erasure or return of Personal Information**.

   a. Certn shall only Process the Personal Information provided by the Client during the Term of the Agreement.

   b. Unless otherwise agreed between the Parties, the provisions in Annex I.B shall apply in relation to the data retention and erasure schedules.

6. **Security of Processing.**

   a. Certn shall maintain commercially reasonable standards to ensure the security of the Personal Information, including protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (personal data breach). A copy of Certn's technical and organizational measures are set out in Annex II. If the Processing involves Personal Information revealing sensitive or biometric data for the purpose of uniquely identifying a natural person, or data relating to criminal convictions and offences, Certn shall apply specific restrictions and/or additional safeguards as reasonably required by the Client from time to time.

   b. In assessing the appropriate level of security, both Parties shall take due account of the risks involved in the Processing, the nature of the Personal Information and the nature, scope, context and purposes of Processing.

   c. In the event of a Personal Information breach, either Party shall notify the other without undue delay, and at the latest within 24 hours, after having become aware of the breach. Such notification shall contain the details of a contact point where more information concerning the Personal Information breach can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and data records concerned), its likely consequences and the measures taken or proposed to be taken to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall be provided as it becomes available without undue delay.

7. **Consumer rights.** Certn shall promptly notify the Client if it receives a Data Subject Access Request. Client shall be responsible for responding to Data Subject Access Requests and, however, to the extent the Client, does not have the

ability to address a Data Subject Access Request, Certn, shall, where required by law or upon the Client's request, provide reasonable efforts to assist the Client in responding to such Data Subject Access Request without additional costs during the timeframe of the Applicable Law.

8. **Subprocessors**.

a. Certn's Sub-processors (found **here**) shall be the entities engaged by Certn who agree to receive Personal Information from the Processor exclusively for Processing activities to be carried out on behalf of the Client's instructions. The Client acknowledges and agrees that Certn's Affiliates (a) may be retained as Sub-processors; and (b) may each engage third-party Sub-processors in connection with the provision of the Services. Certn may remove, replace, or appoint suitable and reliable further Sub-processors, with notice to the Client, at its own discretion.

b. Notwithstanding the above, Client may reasonably object to Certn's use of a new Sub-processor, for reasons relating to the protection of Personal Information intended to be Processed by such Sub-processor, by notifying Certn promptly in writing within three (3) business days after receipt of Certn's notice. Such written objection shall include those reasons for objecting to Processor's use of such a new Sub-processor. Failure to object to such a new Sub-processor in writing within three (3) business days following Certn's notice shall be deemed as acceptance of the new Sub-Processor. In the event the Client reasonably objects to a new Sub-processor, as permitted above, Certn may:

i. stop using the Sub-processor with regard to the Personal Information submitted by the Client;

ii. take the corrective steps as requested by the Client in its objection;

iii. cease to provide (temporarily or permanently) the particular aspect of the Service that would involve the use of such Sub-processor with regard to the Personal Information submitted by the Client; and

iv. provide Client with a written description of commercially reasonable alternative(s), if any, to such engagement, including without limitation modification to the Services.

c. If Certn, in its sole discretion, cannot provide any alternative(s) listed above, or if the Client does not agree to any such alternative(s) if provided, Certn and the Client may terminate the Agreement in accordance with the terms of the Agreement. Termination shall not relieve Client of any fees owed to Certn under the Agreement. Until a decision is made regarding the new Sub-processor, Certn may, where necessary, temporarily suspend the Processing of the affected Personal Information and/or suspend access to the account and Client will have no further claims against Processor due to the temporary suspension or the termination of the Agreement (including, without limitation, requesting refunds).

d. Certn shall ensure that all authorized Sub-processors have executed confidentiality agreements that prevent them from unauthorized Processing of Client Personal Information both during and after their engagement by Certn. In addition, Certn shall, (e.g., by way of contract or other legal act) impose on the Sub-processor the same data protection obligations as set out in this DPA.

9. **International Data transfers.**

a. **International data transfers subject to the SCCs.** Where the transfer of Personal Information is made subject to the SCCs, the "data importer" thereunder shall be either the Processor or its Sub-processor, as the case may be and as determined by Processor, and the "data exporter" shall be the Controller of such Personal Information. The Processor shall ensure that the relevant Sub-processor shall (where applicable) comply with the data importer's obligations, and the Controller shall comply with the data exporter obligations, in each case under the applicable SCCs.

b. **International data transfers from and to countries that offer adequate level of data protection.** Personal Information may be transferred from EU Member States and the EEA member countries (Norway, Liechtenstein, and Iceland) (collectively, "EEA") to countries that offer an adequate level of data protection (including Canada) under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA or the European Commission ("Adequacy Decisions"), as relevant and applicable , without any further safeguard being necessary.

c. **Transfers from Switzerland.** To the extent that the Swiss Supervisory Authority considers the SCCs to provide appropriate safeguards for the purposes of transferring Personal Information and the data of legal entities, the following amendments shall apply in relation to Swiss transfers:
    i. the Parties adopt the GDPR standard for all data transfers;
    ii. in relation to Clause 13a, the EU Supervisory Authority shall be competent insofar as the data transfer is governed by the GDPR and the Swiss Supervisory Authority (FDPIC) shall conduct parallel supervision as applicable; and
    iii. in relation to Clause 18 c, the term 'member state' shall be interpreted in such a way as to allow data subjects in Switzerland with the possibility of suing for their rights in their place of habitual residence (Switzerland).

d. **Transfers from the United Kingdom.** To the extent that the UK Supervisory Authority (the Information Commissioner) considers the SCCs to provide appropriate safeguards for the purposes of transferring Personal Information to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors, the following amendments shall apply in relation to UK transfers:
    i. "The details of the transfers(s) and in particular the categories of Personal Information that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer."
    ii. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws. In particular:
        1. References to Regulation (EU) 2018/1725 are removed;
        2. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK";
        3. Clause 13(a) is not used and the "competent supervisory authority" is the Information Commissioner;
        4. Clause 17 is replaced to state "These SCCs are governed by the laws of England and Wales";
        5. Clause 18 is replaced to state: "Any dispute arising from these SCCs shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and
        6. The footnotes to the SCCs do not apply to UK transfers.

10. **Miscellaneous**. Data Controller shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Data Processor to protect the Data Processor against additional risks associated. If Data Controller proposes any other variations to this DPA which Data Controller reasonably considers to be necessary to address the requirements of Applicable laws, the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations as soon as is reasonably practicable. Notwithstanding the foregoing, upon notice to the Client, Certn may revise this Addendum so as to incorporate any mandatory SCCs or other terms that are required by any competent data protection authority in the EU or the UK.

ANNEX I

Annex I.A - PARTIES

The Data Exporter	The data exporter is identified as the Client or the "Controller" in the DPA.
The Data Importer	The data importer is Certn, a provider of data verification and background screening services.

Annex I.B - PROCESSING INFORMATION

Data Subjects	Those individuals and applicants subject to the background verification services for the purposes of employment, tenancy or any other lawful and permissible purpose as instructed by the Controller.
Categories of Personal Data Transferred	**Client data**: business related contact details (email, phone, email address, names, job titles, business address). **Consumer data**: Email addresses, names, contact details, job titles, residential or business address; photograph; personal identification numbers (where applicable); academic title and qualifications; career history; driving license; attendance records; job title; gender; professional telephone number (including mobile telephone number) and fax number; personal email address; personal telephone number (including mobile telephone number); credit score or limit, risk, failure and delinquency score; payment information; criminal history; records for associated claims and judgments; public records such as directorships, insolvencies, bankruptcies, financial standing, IP address; cookie data; login credentials (username and password); traffic data; images and sounds; Biometric data.
The Frequency of Transfers	Transfers will be processed on an on-demand basis.
Nature of the Processing	The nature and purpose of processing means any operation such as collection, recording, organization, structuring, storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction of data (whether or not by automated means)
Purpose(s) of the Data Transfer and Further Processing	Providing the Services to the Client as set out with the Agreement; performing the Agreement, this DPA and/or other contracts executed by the Parties; providing support and technical maintenance, if agreed in the Agreement; preventing, mitigating and investigating the risks of data security incidents, fraud, error or any illegal or prohibited activity; complying with applicable laws and regulations; all tasks related with any of the above.
The Period for Which the Personal Data Will Be Retained, or, If That Is Not Possible, the Criteria Used to Determine that Period	The Parties agree to erase Personal Data from any computers, storage devices and storage media as soon as practicable after it has ceased to be necessary for such Party to retain the Personal Data under applicable Data Protection Legislation or as otherwise required by the Agreement. Notwithstanding the foregoing, unless otherwise agreed between the Parties, or required under applicable Data Protection Legislation, the Parties agree that (i) Client records will be retained by Certn in accordance with Certn's Retention Policy which may be updated from time to time.

Annex I.C - COMPETENT SUPERVISORY AUTHORITY

Competent Supervisory Authority	Data Protection Commission, the Republic of Ireland.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The Technical and Organizational Measures Implemented by the Data Importer	SOC2 compliance report is available upon request. SOC 3 compliance report is publicly available.
Measures of Pseudonymization and Encryption of Personal Data	The employed level of encryption is AES 256.
Measures For Ensuring Ongoing Confidentiality, Integrity, Availability and Resilience of Processing Systems and Services	Certn is SOC2 and SOC3 certified on a continuous basis.
Measures For Ensuring the Ability to Restore the Availability and Access to Personal Data in a Timely Manner in the Event of a Physical or Technical Incident	Backup and data restore procedures are defined and documented as Certn policies, available upon request. Execution of backups is monitored to ensure completeness. Certn stores data on AWS cloud which has automatic backups configured and encrypted. In addition, there are multiple zones for redundancy and recovery purposes.
Processes for Regularly Testing, Assessing and Evaluating the Effectiveness of Technical and Organizational Measures in Order to Ensure the Security of the Processing	Certn is compliant to and certified under SOC2 and SOC3. Some of the processes and measures ensuring security of processing include, but are not limited to, vulnerability management, risk evaluation, asset management, IDS and IPS, patch management, endpoint monitoring, SIEM tools vendor management.
Measures for User Identification and Authorization	An access control system applicable to all users accessing the IT system has been implemented. The system allows Certn to create, approve, review, and delete user accounts. Certn implements multi-factor authentication for all accounts that have access to Personal Data. Where authentication mechanisms are based on passwords, the data processor requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability. Role- based authorizations in alignment to an established Authorization Control Policy. When granting access or assigning user roles, the “need-to-know principle” is observed in order to limit the number of users having access to Personal Information only to those who require it for achieving the Processor’s Processing Purposes.
Measures for the Protection of Data During Transmission	The Supplier maintains access controls to ensure role based access, logging mechanisms to show events of users which can be ported to a SIEM, encryption of data at rest and in transit using AES 256 encryption and ≥TLS v1.2 respectively.
Measures for the Protection of Data During Storage	Certn maintains a Data Encryption Policy, Data Backup Policy and a Data Retention Policy which govern access, availability and duration of stored categories data.
Measures for Ensuring Physical Security of Locations at which Personal Data is Processed	Certn maintains a Physical Security Policy which covers provisions for physical office access with key fobs, security alarms, security surveillance, visitor limited access. The physical perimeter of the IT system infrastructure is not accessible by non-authorized personnel. Appropriate technical measures and organizational measures are set in place to protect security areas and their access points against entry by unauthorized persons. Certn stores its data on

	AWS cloud following the best practices and requirements. Data is segmented, encrypted and backed up with the inclusion of multi zonal availability.
Measures for Ensuring Events Logging	SIEM collects events and policies and alerts are created for analysis and investigations. Endpoint protections and monitoring, intrusion detection and prevention with monitoring and evaluation .
Measures for Ensuring System Configuration, Including Default Configuration	Certn maintains an Asset Management Policy which defines the Configuration standards and any applicable variables. A system access control policy has been defined, documented and implemented to allow for evaluation of controls and access to Certn's assets.
Measures for Internal IT and IT Security Governance and Management	Certn maintains an Information Security Policy and conducts employee security internal security training during the onboarding phase and annually thereafter.
Measures for Certification/assurance of Processes and Products	SOC2 compliance report is available upon request. SOC 3 compliance report is publicly available.
Measures for Ensuring Data Minimization	Any processed Personal Information is limited to the strictly necessary matching identifiers defined by the data sources we operate with.
Measures for Ensuring Data Quality	To ensure that Personal Information Is accurate, relevant, complete and up-to-date, Certn processes data verifications in real time, with the consent of the Data Subject and only within the limits of the defined Permissible Purpose. Any potentially incomplete data is reconfirmed with the Data Subject and/or the relative data source.
Measures for Ensuring Limited Data Retention	Certn has an established policy for Data Retention which defines different purging schedules for separate categories of data.
Measures for Ensuring Accountability	Certn maintains a "privacy by design approach" and is regularly and independently audited for the purposes of maintaining the highest industry standards for internal controls for security, availability, processing integrity and confidentiality and privacy.
Measures for Allowing Data Portability and Ensuring Erasure	Data Subjects can log Data Subject Access requests which are reviewed by a privacy officer.
Subprocessors	Sub Processors are required to meet the same standards as set out in the current Annex II.