Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of and is incorporated into the Agreement between Company and you (the "**Client**") (collectively the "Parties" and individually the "**Party**") when you created your account. In the event of any conflict between this DPA and the Agreement, this DPA shall control solely with respect to the Processing of Personal Information. This DPA shall be effective as of the Effective Date of the Agreement and shall be effective until the later of, the termination of the Agreement or until deletion or return of all Personal Data as instructed by either Party under this DPA.

1. DEFINITIONS

Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. In the event Data Protection Legislation exists in a jurisdiction, the definitions set forth therein will supersede those herein when such Data Protection Legislation contemplates the terminology.

1.1 "**Agreement**" means any agreement between Company and Client for the Services. Such an agreement may have various titles, such as "Order Form", "Terms of Service", "Service Agreement" or similar titles.

1.2 "**Business Contact Information"** means business related contact details (email, phone, email address, names, job titles, business address).

1.3 "**Client**" means the customer of Company, either through an Agreement with a customer of Company or an Agreement with an individual person.

1.4 "**Client Account and Usage Data**" means information about Client that Client provides to Company in connection with the creation and administration of an account, such as first and last name, username, email address, and billing and payment information of individuals associated with an account. For avoidance of doubt, statistical data, analytical data, individual session data, and anonymized data is not included in this definition.

1.5 "**Company**" means Certn Holdings Inc. and its wholly owned subsidiaries and affiliates including Certn (Canada) Inc., Certn (USA) Inc., Certn (UK) Ltd., InterCheck Global Pty. Ltd., Trustmatic s.r.o., and any affiliates identified in the Sub-Processor List available in Company's Trust Center, (https://trust.certn.co/).

1.6 "**Controller**" means a legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing Personal Data and gives instructions regarding Processing activities.

1.7 "**Corporate Clients**" means Clients of Company that are a registered business entity.

1.8 "**Data Subject Request**" means any request by a natural person (the "Data Subject") to access, update, revise, correct, delete, object to Processing Personal, or any similar request, made pursuant to the applicable Data Protection Legislation.

1.9 "**Data Protection Legislation**" means all laws, rules or regulations applicable to the Agreement, the Services, Company or Client, and applicable industry standards concerning privacy, data protection, confidentiality, information security, availability and integrity, or the handling or Processing (including retention and disclosure) of Personal Data, as may be amended, restated or replaced from time to time.

1.10 "**Personal Data**" or "**Personal Information**" means all information obtained by Company from or on behalf of Client, or Company's Sub-Processors, in any form or format, that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to, an identified or identifiable natural person.

1.11 "**Process(es)**", "**Processing**" or "**Processed**" means any operation or set of operations that is performed upon any Personal Data, whether or not by automatic means, including, but not limited to, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deletion, erasure, or destruction.

1.12 "**Processor**" means the Party to this Agreement, or under an agreement with substantially the same requirements as this DPA, that Processes Personal Data subject to the direction of the Controller and applicable Data Protection Legislation.

1.13 "**Sell**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for monetary or other valuable consideration.

1.14 "**Services**" means those services that Company performs pursuant to the Agreement.

1.15 "**Standard Contractual Clauses**" or "**SCCs**" means (a) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); (b) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022 ("UK SCCs"); and (c) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs"), each as may be updated from time to time.

1.16 "**Sub-Processor**" or "**Service Provider**" means a third-party engaged and supervised by a Party to this Agreement, who agrees to receive and Process Personal Data under the terms of this DPA, or under an agreement with the same requirements as this DPA, solely for the purposes of Processing or delivering Personal Data necessary for the fulfillment of this Agreement. Company Sub-Processor List can be found in Company's Trust Center, (https://trust.certn.co/).

1.17 "**System**" means any system, network, platform, database, computer, or telecommunications or information system owned, controlled, or operated by or on behalf of either Party or any of its affiliates for the purpose of Processing Personal Data pursuant to the Agreement.

2. ROLES OF THE PARTIES

2.1 To the extent that Client's Personal Data is Processed by Company, the Parties agree that Client is the Controller, Company is the Processor.

2.2 To the extent that Company's Personal Data is Processed by Client, the Parties agree that Company is the Controller and Client is the Processor.

2.3 Notwithstanding the preceding, each Party agrees that it is the Controller of the other Party's Business Contact Information that the Party Processes in relation to the Agreement.

3. PROCESSING OF PERSONAL DATA

Company agrees to:

3.1. Process Personal Data solely as necessary to provide the Services to Client, and in accordance with Data Protection Legislation, the Agreement, this DPA including Annex I and Annex II, and any additional written instructions provided by Client;

3.2. refrain from (i) selling or sharing Personal Data (ii) retaining, using or disclosing the Personal Data for any purpose other than for the purpose specified in the Agreement, (iii) retaining, using or disclosing the Personal Data outside of the direct relationship between Company and Client, and (iv) combining Personal Data from different sources unless necessary for the provision of Services under this Agreement.

3.3. maintain the confidentiality of all Personal Data and ensure that its personnel, including employees, interns, temporary workers, and agency workers, have executed confidentiality agreements that prevent them from unauthorized Processing of Personal Data for the duration of their engagement with Client.

3.4. not disclose Personal Data to third parties, including government agencies unless required by law, and Sub-processors except for the provision of Services under this Agreement.

3.5. when required by Data Protection Legislation promptly notify (email acceptable) Client of:

3.5.1 any request, inquiry, complaint, notice, or communication received from any third party, including a Data Subject or a supervisory authority, with respect to any Personal Data and comply with instructions of Client in responding to such request, inquiry, complaint, notice, or communication. Client agrees to respond to Company's notification within ten (10) business days. Client agrees that if it fails to respond to Company's notification, Company may, in its reasonable judgment, determine how to processed with the Data Subject or supervisory authority's request;

3.5.2. any request for the provision of Personal Data to a government body or authority or court, whether through legal means or otherwise, including specific details of the data provided, unless prohibited by law or legal order;

3.5.3. any instruction by Client that Company believes to be in violation of Data Protection Legislation prior to engaging in the relevant Processing; and

3.5.4. any substantial changes to the Company's notices, policies, or procedures that would impede Company's ability to

fulfill the terms of this DPA regarding protection of Personal Data.

3.6. as is allowed by Data Protection Legislation and limited to Corporate Clients, upon written request, submit the databases, tools, office space (if applicable), and other similar cloud based or on premises environments or locations used by Company to Process Personal Data for audit in accordance with any audit provision that may be available under the Agreement and *Section 9. Information Requests* below. For avoidance of doubt, any audit rights available to Client is limited in scope to the Services directly provided to Client under this Agreement.

3.7. keep records that demonstrate its compliance with its obligations under this DPA, and reasonably make them available to Client upon request and/or in connection with any audit referred to in Section 3.6 above and Section 9. Information Requests below.

3.8. reasonably assist and cooperate with Client, including by providing information requested by Client, to allow Client to comply with its obligations under Data Protection Legislation, including the certification of Company's completion of transfer impact assessments, privacy impact assessments, and data protection impact assessments; and

3.9. retain Personal Data in accordance with Section 6. Data Retention of the Agreement and *Section 8. Deletion or Return of Personal Data* of this DPA, but in no event longer than necessary to perform the Services.

4. INFORMATION SECURITY MEASURES

Company represents and warrants that it has established, maintains and complies with:

4.1. administrative, technical, and physical safeguards designed to ensure the security, confidentiality, reliability, and integrity of Personal Data, as well as any Systems, facilities, or software that Company accesses or supports in connection with the Agreement. Such safeguards are:

4.1.1. commensurate with the type and volume of Personal Data Processed by Company, having regard to the state of the art and industry standards, and should, at minimum, protect Personal Data and Systems against reasonably anticipated threats or hazards, including from unauthorized access, loss, theft, destruction, use, modification, collection, attack, or disclosure;

4.1.2. in accordance with globally recognized security control standards such as ISO; and

4.1.3. compliant with applicable specific industry standards as may apply to the Personal Data being Processed by Company.

4.2. a written security program and policies that meet or exceed the requirements imposed under Data Protection Legislation and align with established industry practices. Such security program and policies address, at a minimum, the following:

4.2.1. identification of appropriately defined organizational roles related to information security;

4.2.2. controls with respect to employment of and access given to Personal Data by employees, agents and subcontractors of Company including background checks, training regarding the handling of Personal Data, and when applicable, security clearances that assign specific access privileges to individuals;

4.2.3. an appropriate network security program that includes, without limitation, encryption and network and application partitioning;

4.2.4. access identification and authentication;

4.2.5. maintenance and media disposal;

4.2.6. audit and accountability;

4.2.7. physical and environmental protections;

4.2.8. system and communication security;

4.2.9. incident response and planning; and

4.2.10. the integrity and reliability of facilities, systems and services, including critical asset identification, configuration and change management for software systems, and contingency planning/redundancy.

4.3. If Personal Data being Processed includes sensitive or biometric data for purposes of uniquely identifying a natural person, or data relating to criminal convictions and offenses, Company shall apply specific restrictions and/or additional safeguards in compliance with Data Protection Legislation. Client agrees that Company may implement adequate alternative security measures from time to time, provided the security level of the alternative measures is not materially decreased.

4.4. Company shall limit access to Personal Data to those individuals who require access to the Personal Data to meet Company obligations with respect to the delivery of the Services to Client. Company shall ensure that those individuals are informed in writing of the confidential or sensitive nature of the Personal Data.

5. DATA SECURITY INCIDENT

5.1. Data Security Incident means (i) the loss or misuse (by any means) of Personal Data; (ii) the inadvertent, unauthorized, and/or unlawful disclosure, access, alteration, corruption, transfer, sale, rental, destruction, or use of Personal Data; or (iii) any other act or omission that compromises or may compromise the security, confidentiality, or integrity of Personal Data or a System.

5.2. If Company suspects or becomes aware of a Data Security Incident, Company will:

5.2.1. Notify client without undue delay, and in any case within seventy-two (72) hours, after it becomes aware of any confirmed Data Security Incident;

5.2.2. Undertake an investigation of such Data Security Incident and respond to Client's reasonable requests for information relating to the Data Security Incident as may be necessary;

5.2.3. Reasonably assist Client, its regulators and law enforcement agencies, with notification obligations under the applicable Data Protection Legislation. Unless otherwise required in accordance with applicable laws, Client and shall be solely responsible for complying with any Data Protection Legislation data breach notification requirements applicable to Client and fulfilling any third-party notification obligations related to any Data Security Incident; and

5.2.4. Take all reasonable corrective action in a timely manner, at the expense of Company, to remediate and prevent a recurrence of such Data Security Incident.

6. SUB-PROCESSORS

6.1. Client hereby grants general written authorization to Company to appoint Sub-Processors to perform specific Processing activities on its behalf. A list of Sub-Processors currently engaged by Company in connection with the Services is available in Company's Trust Center, (https://trust.certn.co/).

6.2. Company will provide notice on its website of a new Sub-Processor via (https://trust.certn.co/). Client should review the Sub-Processor List from time to time to stay up to date regarding Company's Sub-processors.

6.3. When required by Data Protection Legislation, and limited to Corporate Clients, Company will provide written notice (email sufficient) of a new Sub-Processor. Business Client has a right to reasonably object to Company's use of Sub-processor. Instructions for the objection of Sub-Processor's is available in Company's Trust Center, (https://trust.certn.co/). If, as a business Client, an objection is raised, Company will use reasonable efforts to find an alternative Sub-Processor to perform the specific Processing activities. If a suitable alternative Sub-Processor or other solution cannot be found, then Client may terminate the relevant part of the Agreement to which the Sub-Processors services relate.

6.4. Company warrants that any Sub-Processor engaged by Company to Process Personal Data under this Agreement has:

6.4.1. provided appropriate safeguards and maintains adequate level of protection in relation to the processing and transfer of Personal Data;

6.4.2. entered into a written agreement with Company, which encompasses substantially similar terms to this Agreement, particularly containing the same data protection obligations as set out in this Agreement; and

6.4.3. established the appropriate mechanisms to ensure any Data Subject has enforceable rights and effective legal remedies.

6.5. Company acknowledges that as a Processor, it is liable to Corporate Clients for Company's Sub-Processor's compliance

with its data protection obligations as they apply to processing of Personal Data Processed under the Agreement and this DPA.

7. INTERNATIONAL DATA TRANSFERS

7.1. **General**. The Parties agree that in the event a jurisdiction does not currently have Data Protection Legislation that contemplates data transfers outside of the country, such transfers will be subject to the standards and expectations imposed by the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR") and thereby subject to the EU Standard Contractual Clauses ("EU SCCs"), including transfers between Company and its Sub-Processors. By signing this DPA, Client hereby authorizes Company to enter into the EU SCCs for and on Client's behalf (as exporters) with Company's own affiliates and Sub-Processors, in order to ensure an adequate level of protection to Personal Data as required by Data Protection Legislation. In case of any conflict between this DPA and such EU Standard Contractual Clauses, the EU Standard Contractual Clauses shall prevail to the extent necessary to comply with Data Protection Legislation.

7.2. **Processing in and Data Transfers to Sanctioned Jurisdictions.** In connection with the performance of this DPA and the Agreement, Client authorizes Company to Process and transfer Personal Data from Company's jurisdiction, if necessary, to any jurisdiction in which Company or its Sub-Processors are located, so long as those receiving jurisdictions are not currently sanctioned by the Office of Foreign Assets Control (OFAC) or similar country sanction lists in Canada, United Kingdom, or Australia, and to any other country that is recognized by the European Commission as providing an adequate level of protection for Personal Data.

7.3. **Data Transfers from the European Economic Area Subject to the EU Standard Contractual Clauses.** Where the transfer of Personal Data is made subject to the EU GDPR and thereby subject to the EU 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 or Controller-Processor of such Personal Data. 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.

7.3.1. Company will be a Processor of Personal Data;

7.3.2. Client will be a Controller of Personal Data;

7.3.3. Module 2 (Controller to Processor) shall apply;

7.3.4. Clause 7 (Docking Clause) shall apply;

7.3.5. The parties choose Option 2 of Clause 9;

7.3.6. The option in Clause 11(a) (Redress) Module 2 shall apply;

7.3.7. The parties choose Option 1 of Clause 17, the law of Ireland shall apply; and

7.3.8. For purposes of the Standard Contractual Clauses, Annex I and Annex II shall be incorporated and meet the standards as set forth in the EU GDPR.

7.4. **Data Transfers from and to countries that offer adequate levels of data protections.** 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.

7.5. **Data Transfers from Switzerland**. Company adheres to Switzerland's revised Federal Data Protection Act (revFADP). 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).

7.6. **Data 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 organization 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:

7.6.1. 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 Section B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.

7.6.2. 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:

7.6.2.1. References to Regulation (EU) 2018/1725 are removed;

7.6.2.2. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK";

7.6.2.3. Clause 13(a) is not used and the "competent supervisory authority" is the Information Commissioner;

7.6.2.4. Clause 17 is replaced to state "These SCCs are governed by the laws of England and Wales";

7.6.2.5. 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

7.6.2.6. The footnotes to the SCCs do not apply to UK transfers.

7.6.2.7. Company will be a Processor of Personal Data;

7.6.2.8. Client will be a Controller of Personal Data;

7.6.2.9. Module 2 (Controller to Processor) shall apply; 7.6.2.10.Clause 7 (Docking Clause) shall apply;

7.6.2.11. The parties choose Option 2 of Clause 9.

7.6.2.12. The option in Clause 11(a) (Redress) model 2 shall apply;

7.6.2.13.The parties choose Option 1 of Clause 17, the law of England and Wales shall apply; and

7.6.2.14.For purposes of the UK Addendum, Annex I and Annex II shall suffice and meet the necessary requirements under UK Data Protection Laws.

7.7. **Data Transfer from the EEA, UK, or Switzerland to the United States**. Data transfer from the EEA, UK or Switzerland may be deemed adequate when done so under the EU-U.S. Data Privacy Framework or Swiss-U.S. Data Privacy Framework. These frameworks between the United States Department of Commerce, European Commission, UK government, and Swiss Federal Administration solely apply to commercial entities who are actively registered with the U.S. Department of Commerce's Data Privacy Framework Program, to allow Personal Data to be transferred from the European Union under the European Commission's adequacy decision.

7.8. **Data Transfer from the Canadian Province of Quebec**. Where the transfer of Personal Data relating to a resident of the Canadian Province of Quebec and thereby made subject to the Act respecting the protection of personal information in the private sector (the "Private Sector Act"), Company conducts a transfer impact assessment in accordance with the Private Sector act to determine that such transfer to its Sub-Processor, shall have adequate levels of protection commensurate to the nature and volume of the Personal Data, including but not limited to those standards and expectations set forth in this Agreement.

8. DELETION OR RETURN OF PERSONAL DATA

8.1. Upon the expiration or earlier termination of the Agreement, and upon Client's request, Company will delete or return, at Client's election, all Personal Data in the possession or control of Company and Company's Sub-Processors, unless the continued retention of such Personal Data is required by applicable law.

8.2. Without limitation to the generality of the foregoing, and upon written request, Company and Company's Sub-Processors shall, within thirty (30) days of a written request from Client, or as a result of a suspension of transfer of Personal Data, provide a copy of the Personal Data in a portable and readily useable format.

9. INFORMATION REQUESTS

9.1. In accordance with the Agreement, Company agrees to reasonably cooperate with Corporate Clients to provide Corporate Clients with such information that is reasonably necessary to enable Corporate Clients to demonstrate compliance with the obligations set forth in this DPA and allow for and contribute to audits, including inspections, conducted by Corporate Client or a qualified independent third-party assessor who is reasonably acceptable to Company and bound by confidentiality obligations satisfactory to Company, to the extent that such information is within Company's control and Company is not precluded from disclosing it by applicable law, a duty of confidentiality, a legal privilege or protection, or any other obligation owed to a third party. Audits and inspections are subject to a thirty-day (30) written notice, shall be

conducted at the Client's expense, and no more than once per every twelve (12) months during the term of the Agreement, and during regular business hours.

9.2. Company agrees to, taking into account the nature of the processing and the information available to Company, reasonable assist Corporate Clients in meeting its obligations described by appliable Data Protection Legislation to keep Personal Data secure by maintaining reasonable security standards as set forth in this DPA; reasonably assist Corporate Clients in notifying the applicable regulatory or supervisory authority, including the Information Commissioner's Office ("ICO"), of Personal Data breaches; reasonably assist in notifying Data Subjects of Personal Data breaches; reasonably assist Corporate Clients in carrying out data protection impact assessments (DPIAs) when required, and at Corporate Client's expense reasonably consult ICO where a DPIA indicates there is a high risk that cannot be mitigated.

10. ASSIGNMENT AND SUCCESSORS

Client may not assign any of its rights or obligations under this DPA without the prior written consent of Company, such consent will not be unreasonably withheld. Subject to the foregoing, the rights and obligations under this Agreement shall ensure to the benefit of and are binding on Client and their permitted assignees, transferees and successors. Any attempted assignment in violation of this clause is void. Notwithstanding the foregoing, Company shall have the right to assign any of its right or obligations under this DPA.

11. COMPANY NOTICE CONTACT INFORMATION

11.1. Notice relating to Data Security Incidents must be sent to the following:

To:Security

CC: Privacy@certn.co and Legal@certn.co

11.2. Notice relating to Data Subject Rights Requests and Sub-Processor updates must be sent to the following:

To: Privacy@certn.co

11.3. Notices relating to Government Agencies or Regulatory Bodies Disclosure Requests:

To: Legal@certn.co

CC: Privacy@certn.co

11.4. All other notices relating to this DPA must be sent to the following:

To: Privacy@certn.co

CC: Legal@certn.co

ANNEX I
Section A: List of 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.

Section B: Description of Processing and Transfer

1. Categories of data subjects whose personal data is transferred
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.

2. Categories of Personal Data Transferred
Business Contact Information: Has the meaning provided in section 1.2 of the DPA.

Data Subject Personal Data: The exact Data Subject Personal Data will vary depending on the requested background verification service, but may include the following, as required: Email addresses, names, contact details, job titles, residential or business address; photograph; personal identification numbers; 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.

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The contents of the Personal Data are varied and under the Data Exporter's control, but may, depending on the particular Services, include sensitive data as defined under the relevant Data Protection Legislation. Sensitive Personal Data will be protected in accordance with the measures set out in the DPA.

4. The Frequency of Transfers
Transfers will be processed on an ad hoc basis and for the duration necessary for the performance of the Services; any other purposes stipulated in the Agreement; and complying with applicable laws and regulations.

5. 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).

6. 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.

7. 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 Client records will be retained by Company in accordance with Company's Retention Policy which may be updated from time to time.

Personal Data collected and processed as part of a Disclosure and Barring Service ("DBS") check is retained for a minimum period of two (2) years in accordance with applicable guidelines.

8. For transfers to (sub-) processors, also specify the subject matter, nature, and duration of the processing

All authorized sub-processors are required to implement and maintain the same or substantially similar technical and organizational measures, responsibilities, and obligations as those required of Provider under this DPA.

Section C: Competent Supervisory Authority

1. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as a competent supervisory authority.

2. Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established will act as the competent supervisory authority.

3. Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without, however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: Data Protection Commission (DPC) – 21 Fitzwilliam Square, South Dublin 2, D02 RD28 Ireland will act as the competent supervisory authority.

4. Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office will act as the competent supervisory authority.

5. Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner will act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

6. Where the data exporter is established in the Canadian Province of Quebec or falls within the territorial scope of application of Quebec Data Protection Laws, the Commission d'accès à l'information du Quebec will act as the competent supervisory authority.

ANNEX II

Below are the technical, physical and administrative measures used by Company to ensure the security of Personal Data.

1. **Program**. Company maintains a written information security program ("Information Security Program"), which contains reasonably appropriate administrative, technical, and organizational safeguards that comply with this Annex II. Company maintains conducts internal security training during the onboarding phase and annually thereafter.

2. **Security Certifications**. Company maintains ISO 27001, SOC2 and SOC3 certifications on a continuous basis. ISO 27001 and SOC2 compliance report is available upon request. SOC 3 compliance report is publicly available. Visit Company's Trust Center for additional information (https://trust.certn.co/).

3. **Access Controls**. An access control system applicable to all users accessing the IT system has been implemented. The system allows Company to create, approve, review, and delete user accounts.

a. Company 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.

b. 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.

c. Company 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 Company's assets.

4. **Account Management**. Company manages the creation, use, and deletion of all account credentials used to access the Company's key infrastructure, including by requiring multi-factor authentication in all critical systems. Any processed Personal Information is limited to the strictly necessary matching identifiers defined by the data sources we operate with. To ensure that Personal Information Is accurate, relevant, complete and up-to-date, the Company 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 relevant data source.

5. **Vulnerability Management.** Company engages in vulnerability management, risk evaluation, asset management, IDS and IPS, patch management, endpoint monitoring, SIEM tools vendor management. 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.

6. **Security Segmentation.** Company will monitor, detect and restrict the flow of information on a multilayered basis using tools such as firewalls, proxies, and network-based intrusion detection systems.

7. **Data Loss Prevention.** Company uses loss prevention measures to identify, monitor, and protect Personal Data in use, in transit, and at rest. Such data loss prevention processes and tools will include: (a) automated tools designed to identify attempts of data exfiltration; and (b) the use of encryption certificate-based security. Backup and data restore procedures are defined and documented as Company policies, available upon request at Company's Trust Center (https://trust.certn.co/). Execution of backups is monitored to ensure completeness. Company stores data on AWS cloud which has automatic backups configured and encrypted. In addition, there are multiple zones for redundancy and recovery purposes.

8. **Encryption**. Company will encrypt, using industry-standard encryption tools, all Personal Data that Provider transmits across

public networks. Company deploys encryption of data at rest and in transit using AES 256 encryption and ≥TLS v1.2.

9. **Pseudonymization**. Company, where possible and consistent with the Services, uses pseudonymization techniques to protect Personal Data.

10. **Product Development Safeguards**. Company utilizes a privacy and security 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.

11. **Physical Safeguards.** Company maintains physical access controls to secure the Company-owned physical premises where the relevant Company computing environment used to Process any Personal Data is located, including an access control system that enables Company to control physical access to each Company facility. Company maintains a Physical Security Policy which covers provisions for physical office access with key fobs, security alarms, security surveillance, and 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. Company 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.

12. **Administrative Safeguards.** Prior to providing access to Client Personal Data to any of its personnel, Company will use commercially reasonable measures to: (a) verify the reliability of such personnel; and (b) provide appropriate security training to such personnel. Company has an established policy for Data Retention which defines different purging schedules for separate categories of data.