DATA PROTECTION ADDENDUM TO THE ACCREDIBLE CERTIFICATE CLOUD SERVICES AGREEMENT REGARDING THE PROCESSING OF PERSONAL DATA

(hereinafter referred to as "**Accredible DPA**")

by and between

1. EdInvent, Inc., D.B.A. Accredible; Accredible, 800 West El Camino Real, Suite 180, Mountain View, CA 94040 United States

- hereinafter referred to as "**Accredible**" -

and

2. the Accredible customer that is a party to the Cloud Services Agreement

- hereinafter referred to as "**Customer**" -

- **Accredible** and Customer hereinafter referred to as "**Parties**" and each as "**Party**" -

PREAMBLE

Accredible performs cloud-based services to Customer ("**Services**") as agreed between the Parties in the Accredible Certificate Cloud Services Agreement between Customer and Accredible ("**Cloud Services Agreement**").

This Accredible DPA forms part of and is subject to the terms and conditions

of the Cloud Services Agreement. This Accredible DPA regulates the data protection obligations of the Parties when Processing Personal Data under the Cloud Services Agreement and will reasonably ensure that such Processing will only be rendered on behalf of and under the Instructions of Customer.

1. DEFINITIONS

In this Accredible DPA, the following definitions shall apply:

– "**Applicable Law**" means all laws, rules and regulations applicable to either party's performance under this Accredible DPA, including but not limited to those applicable to the Processing of Personal Data. This may include, in particular, the CCPA and/or the GDPR.

–"**Business**" means the entity which determines the purposes and means of the Processing of the Personal Data of California residents.

–"**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq., including any amendments and implementing regulations thereto that become effective on or after the effective date of the Cloud Services Agreement.

–"**Controller**" shall mean the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data of individuals located in the EEA;

–"**Data Subject**" means the individual to whom the Personal Data relates.

–“**EEA**" means the member states of the European Union, Iceland, Liechtenstein, and Norway and, for the purposes of this agreement, the United Kingdom and Switzerland.

–"**GDPR**” means, as applicable, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data repealing Directive 95/46/EC, all national implementing laws validly amending the applicable rules for the Processing of Personal Data under the GDPR, and/or all other applicable data protection laws of the EEA and UK Data Protection Law.

–“**Instruction**” means any documented instruction set forth in the Cloud Services Agreement or submitted by Customer to Accredible in accordance with the standard functionality of the Services that is consistent with the obligations set forth in the Cloud Services Agreement and/or this Accredible DPA, directing Accredible to perform a specific action with regard to Personal Data, including but not limited to the rectification, erasure or restriction of Processing of Personal Data. Instructions shall initially be specified in the Cloud Services Agreement and may, from time to time thereafter, be amended, supplemented or replaced by the Parties by separate written or text form instructions, provided that such instructions still fall within the scope of the Services. Instructions issued for the purpose of complying with statutory claims under the GDPR such as rectification, erasure, restriction or portability of Personal Data fall within the scope of the Services.

–“**Personal Data**” means any Customer Data that is “personal data” or

“personal information” under and regulated by Applicable Laws.

–“**Process**” or “**Processing**” means any operation or set of operations which is performed by or on behalf of Accredible as part of the Services upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

–"**Processor**" shall mean an entity which Processes Personal Data of individuals located in the EEA on behalf of the Controller.

–"**Subprocessor**" shall mean any Accredible Afilliate and any sub-contractor engaged in the Processing of Customer Personal Data in connection with the Services.

–“**Security Incident**” means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Accredible’s possession or control.

–“**Service Provider**” means the entity that Processes Personal Data of California residents on behalf of a Business fora business purpose pursuant to the Cloud Services Agreement.

2. DPA SCOPE

2.1 This Accredible DPA is an integral part of the Cloud Services Agreement with respect to any Processing of Personal Data provided by Customer or

Customer's affiliates who are beneficiaries under the Cloud Services Agreement or any purchase order based thereon (any such affiliate is hereinafter referred to as: "**Affiliate**") as amended from time to time by written agreement between both Parties.

2.2 Notwithstanding anything to the contrary, this DPA will apply only to the extent that Accredible Processes Personal Data falling within the scope of the GDPR or CCPA on behalf of Customer in the course of providing the Services.

2.3 For purposes of and to the extent applicable under this Accredible DPA, Customer and Accredible agree that Customer, and respectively its Affiliate, is the Controller of Personal Data and Accredible is the Processor of Personal Data, except when Customer or Affiliate acts as a Processor of Personal Data, in which case Accredible is a Subprocessor.

2.4 For purposes of and to the extent applicable under this Accredible DPA, Customer and Accredible agree that Customer, and respectively its Affiliate, is the Business with regard to the Processing of Personal Data of California residents, and Accredible is the Service Provider, except when Customer or Affiliate acts as a Service Provider of Personal Data, in which case Accredible is also a Service Provider.

3. SUBJECT MATTER, DURATION, NATURE AND PURPOSE, AND SPECIFICATION OF PROCESSING OPERATIONS

3.1 The subject matter, duration, nature and purpose of the Processing are described in the Cloud Service Agreement and this Accredible DPA.

3.2 The types of Personal Data and categories of Data Subjects that may be affected by the Processing are listed in the Accredible DPA.

3.3 The duration of the Processing shall correspond to the duration of this Accredible DPA as set forth in Sec. 9.

4. ACCREDIBLE'S OBLIGATIONS

4.1 Accredible shall in the course of providing Services, including with regard to transfers of Personal Data to a third country, Process Personal Data to provide the Services on behalf of and under the documented Instructions of Customer unless required to do so otherwise by Applicable Law, including the law of the European Union or the law of a member state of the European Union ("Member State"); in such a case, Accredible shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

4.2 Without limiting the foregoing, Accredible shall not retain, use, sell or disclose Personal Data covered by the CCPA outside of the direct business relationship between the Customer and Accredible, unless otherwise required or permitted by Applicable Law.

4.3 Accredible shall take steps reasonably necessary to ensure that any natural person acting under its authority who has access to Personal Data does not Process such data except on Instructions from Customer, unless otherwise required to do so by Applicable Law.

4.4 Accredible ensures that persons authorized to Process the Personal Data

have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that the obligation will remain after termination of this Accredible DPA.

4.5 Technical and Organizational Data Security Measures

4.5.1 The appropriate technical and organizational data security measures implemented at the date of the signing of this Accredible DPA are specified in Exhibit 1. The measures specified in Exhibit 1 are subject to technical advancements and development .

4.5.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Accredible shall implement and maintain appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, such as those the measures required by Art.32 GDPR. As appropriate, this may include

- the pseudonymization and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; and
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.

4.5.3 When assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

4.5.4 If Accredible significantly modifies measures specified in Exhibit 1, such modifications have to meet the obligations pursuant to Sec.4.5.2 and 4.5.3.

4.6 Accredible shall, while taking into account the nature of the Processing, assist Customer through appropriate technical and organizational measures, with the fulfilment of Customer's obligations to respond to requests for exercising rights of Data Subjects in accordance with Applicable Law, in particular Art. 15 through 18 and 21GDPR.

4.7 Taking into account the nature of the Processing and the information available to Accredible, Accredible shall provide reasonable assistance to Customer in Customer's efforts to ensure compliance with the obligations pursuant to Art.33 through 36GDPR (Data Security Breach Notification, Data Protection Impact Assessment, Consultation with Data Protection Supervisory Authorities).

4.8 Documentation and Audit Rights

4.8.1 Upon request and subject to executing a non-disclosure agreement, Accredible shall provide to Customer a comprehensive documentation of the technical and organizational data security measures it has implemented for Personal Data in accordance with industry standards. In addition, Accredible may, in its discretion, provide data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, by a publicly certified auditing company or by another customer of Accredible.

4.8.2 If Customer has justifiable reason to believe that Accredible is not complying with the terms and conditions under this Accredible DPA, in particular with the obligation to implement and maintain the agreed technical and organizational data security measures, and only once per year (unless the Parties agree there are specific indications that require a more frequent inspection), Customer is, subject to executing a non-disclosure agreement, entitled to audit Accredible in accordance with the terms set forth in this Accredible DPA. This audit right can be exercised by (i) requesting additional information, (ii) accessing the databases which Process Personal Data or (iii) by inspecting Accredible's working premises whereby in each case no access to Personal Data of other customers or Accredible's confidential information will be granted. Alternatively, Customer may also engage third party auditors to perform such tasks on its behalf in accordance with Sec. 4.8.4. The costs associated with such audits and/or for providing additional information shall be borne by Customer.

4.8.3 If Customer intends to conduct an audit at Accredible's working premises, Customer shall give reasonable notice to Accredible and agree with Accredible on the time and duration of the audit. Inspections shall be made during regular business hours and in such a way that business operations are not disturbed. At least one employee of Accredible may accompany the auditors at any time. Accredible may memorialize the results of the audit which shall be confirmed by Customer.

4.8.4 Customer may not appoint a third party as auditor who (i) Accredible reasonably considers to be in a competitive relationship to Accredible or (ii) is not sufficiently qualified to conduct such an audit, or (iii) is not independent.

Any such third-party auditor shall only be engaged if the auditor is bound by a non-disclosure agreement in favor of Accredible prior to conducting any audit.

4.9 Notification Duties

4.9.1 Accredible shall notify Customer without undue delay after becoming aware of a Security Incident. Such notice will, if possible, include the following information:

- a description of the nature of the Security Incident including where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;
- a description of the measures taken or proposed to be taken by Accredible and/or Customer to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects; and
- any further information which is available and known to Accredible and (i) that is necessary for Customer to comply with Customer's notification obligations and (ii) which Customer does not otherwise have access to.

4.9.2 Accredible shall inform Customer immediately if, from its point of view, an Instruction of Customer may lead to a violation Applicable Law. Until Customer either confirms or alternates the Instruction, Accredible may refuse to comply with the Instruction issued.

4.10 Rectification, Erasure, Restriction

4.10.1 If legally required and Customer is unable to perform the applicable task itself, or if provided so in the services description contained in the Cloud Services Agreement, Accredible shall rectify, erase, restrict or transmit Personal Data upon Customer's request as soon as possible but at the latest

within thirty (30)days upon notice. Any erasure of Personal Data pursuant to this Sec.4.10 shall be executed in such a manner that restoring or recovering such data is rendered reasonably impossible.

4.10.2 Unless Applicable Law requires or the parties have otherwise agreed to a retention of the Personal Data, Accredible shall, upon termination or expiration of the Cloud Services Agreement in consultation with Customer, delete all Personal Data all Personal Data in its possession to Customer.

4.10.3 If a Data Subject addresses Accredible with claims for access, rectification, erasure, restriction, objection or data portability of Personal Data, Accredible shall refer the Data Subject to Customer.

4.11 International Transfers of Personal Data

4.11.1 Customer authorizes Accredible and its Subprocessors to transfer Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States.

4.11.2 Accredible agrees that it has provided true, complete, and accurate responses to the Data Transfer Impact Assessment Questionnaire attached hereto as Exhibit 2.5

4.11.3 If Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Customer to Accredible in a country that has not been found to provide an adequate level of protection under Applicable Laws, the Parties agree that the transfer shall be governed by the Standard Contractual Clauses attached hereto as Exhibit 3. The Parties agree that: (i) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Standard Contractual Clauses will be provided upon

Customer's written request; (ii) the measures Accredible is required to take under Clause 8.6(c) of the Standard Contractual Clauses will only cover Accredible's impacted systems; (iii) the audit described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Section 4.8 of the Accredible DPA; (iv) Accredible may engage Subprocessors using European Commission DecisionC(2010)593 Standard Contractual Clauses for Controllers to Processors or any other adequacy mechanism provided that such adequacy mechanism complies with Applicable Laws and such use of Subprocessors shall not be considered a breach of Clause 9 of the Standard Contractual Clauses; (v) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Standard Contractual Clauses will be limited to the termination of the Standard Contractual Clauses, in which case, the corresponding Processing of Personal Data affected by such termination shall be discontinued unless otherwise agreed by the Parties; (vi) unless otherwise stated by Accredible, Customer will be responsible for communicating with Data Subjects pursuant to Clause 15.1(a) of the Standard Contractual Clauses; (vii) the information required under Clause 15.1(c) will be provided upon Customer's written request; and (viii) notwithstanding anything to the contrary, Customer will reimburse Accredible for all costs and expenses incurred by Accredible in connection with the performance of Accredible's obligations under Clause15.1(b) and Clause 15.2 of the Standard Contractual Clauses without regard for any limitation of liability set forth in the Cloud Services Agreement. Each Party's agreement or signature to this Accredible DPA shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

4.11.4 Taking into account the information and obligations set forth in this Accredible DPA and, as may be the case for a Party, such Party's independent

research, to the Parties' knowledge, the Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the attached Standard Contractual Clauses to a country that has not been found to provide an adequate level of protection under Applicable Laws is afforded a level of protection that is essentially equivalent to that guaranteed by Applicable Laws.

4.12 Accredible will inform Customer of the name and the official contact details of its data protection officer if Accredible is, by Applicable Law, required to appoint a data protection officer. If Accredible is not required to appoint a data protection officer, Accredible shall – in its own discretion – name a person responsible for dealing with questions relating to Applicable Law and data security in the context of performing this Accredible DPA.

4.13 In the case claims based on Art.82 of the EU or UK GDPR are raised against Customer, Accredible shall reasonably support Customer with its defense to the extent the claim arises in connection with the Processing of Personal Data by Accredible in connection with performing the Services to Customer.

4.14 Accredible will make available to Customer reasonable information necessary to demonstrate compliance with the obligations laid down in Accredible DPA as required by Applicable Law.

5. CUSTOMER'S OBLIGATIONS

5.1 Customer shall comply with Applicable Law. Customer shall inform Accredible immediately if Processing by Accredible might lead to a violation

of Applicable Law.6

5.2 In the case claims based on Art.82 of the EU or UK GDPR are raised against Accredible, Customer shall reasonably support Accredible with its defense to the extent the claim arises in connection with the Processing of Personal Data by Accredible in connection with performing the Services to Customer or Affiliate.

5.3 Customer shall name a person responsible for dealing with questions relating to Applicable Law and data security in the context of performing this Accredible DPA.

6. SUBPROCESSING

6.1 Customer acknowledges and agrees that Accredible may engage third parties to perform the agreed Processing activities under this Accredible DPA ("**Subprocessors**") subject to the requirements pursuant to this Sec.6 and applicable provisions of GDPR.

6.2 Any Subprocessor with access to Personal Data covered by the GDPR shall be obliged before initiating the Processing, to commit itself in writing to comply with the same data protection obligations as those required by the GDPR unless explicitly agreed otherwise. Where the Subprocessor fails to fulfil its data protection obligations, Accredible shall remain fully liable to Customer for the performance of the Subprocessor's obligations.

6.3 Customer hereby grants general written authorization to Accredible to appoint Subprocessors to perform specific Processing activities on its behalf.

A list of Sub-processors currently engaged by Accredible in connection with the Services, can be accessed in the Subprocessors webpage - https://www.accredible.com/legal/subprocessors (as may be updated by Accredible from time to time in accordance with this DPA). Accredible will inform Customer of any intended changes concerning the addition or replacement of its Subprocessors with access to Personal Data covered by the GDPR. Customer will have an opportunity to object to such changes on reasonably justifiable grounds related to the inability of such Subprocessors to protect Customer Personal Data in accordance with the relevant obligations of this DPA or the applicable data protection regulation, within ten (10) calendar days after being notified. In the case Customer objects to the subprocessing, the Parties will work together in good faith to resolve the grounds for the objection. If Customer does not object to the engagement within the objection period, consent regarding the engagement shall be assumed. Upon Customer's request, Accredible will provide all information necessary to demonstrate that the Subprocessor will meet all requirements pursuant to Sec. 6.2.

6.4 Upon Customer's request, Accredible shall provide Customer with information on relevant data protection obligations of Subprocessor, which may include, but is not limited to, providing a summary of the relevant contractual documents subject to Accredible's confidentiality obligations to its Subprocessors.

7. LIABILITY

7.1 Without any effect as it regards the external liability towards Data Subjects, the Parties agree that not withstanding anything contained hereunder, when

providing the Services, Accredible's liability for breach of any terms and conditions under this Accredible DPA shall be subject to the liability limitations agreed in the Cloud Services Agreement

7.2 No Affiliate shall become beneficiary of the Accredible DPA without being bound by this Accredible DPA and without accepting this liability limitation

8. COSTS FOR ADDITIONAL SERVICES

If Customer's Instructions lead to a change from or increase of the agreed Services or in the case of Accredible's compliance with its obligations pursuant to Sec. 6, 4.10 or 4.13 to assist Customer with Customer's own statutory obligations, Accredible is entitled to charge reasonable fees for such tasks which are based on the prices agreed for rendering the Services and/or notified to Customer in advance.

9. CONTRACT PERIOD

The duration of this Accredible DPA coincides with the duration of the Cloud Services Agreement. It commences and terminates with the provision of the Services under the Cloud Services Agreement, unless otherwise stipulated in the provisions of this Accredible DPA.

10. MODIFICATIONS

Accredible may modify or supplement this Accredible DPA, with notice to Customer, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement standard contractual clauses laid down by the

European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 of the GDPR. Customer shall notify Accredible if it does not agree to a modification, in which case Accredible may terminate this this Accredible DPA and the Cloud Services Agreement with two (2) months' prior written notice, provided that in the case of a Customer objection that is not based on the suggested modifications' non-compliance with Applicable Law, Accredible shall remain entitled to claim its agreed remuneration until the end of the term.

11. WRITTEN FORM

Any side agreements to this Accredible DPA as well as changes and amendments of this Accredible DPA or the Services hereunder, including this Sec.11., shall be in writing and, unless otherwise stated, mutually agreed upon by the Parties.

12. MISCELLANEOUS

12.1 With respect to any issues arising of or in connection with the Processing of Personal Data the Accredible DPA shall prevail over the Cloud Services Agreement between the Parties.

12.2 In the event a clause under the Cloud Services Agreement has been found to violate the GDPR or any other Applicable Laws, the Parties will mutually agree on modifications to the Cloud Services Agreement to the extent necessary to ensure data privacy-law compliant Processing.

Exhibit 1 – Accredible Technical and Organizational Measures

This Exhibit 1 forms part of the Accredible DPA. Capitalized terms not defined in this Exhibit 1 have the meaning set forth in the Accredible DPA.

Any organizational security measures are subject to change as technical standards evolve and such changes can be implemented by Accredible. If so requested, Accredible will provide Customer with a description of the then current measures.

Technical and organizational measures in place by Accredible

1. Access control to premises and facilities:

Physical access to the building is controlled.

Physical access to the office space is monitored, logged and is restricted to individuals who require such access to perform their job responsibilities. Management approval is required before access is granted.

Access to office space requires a key or electronic code and alarm systems are present to prevent unauthorized access.

No on-site data centres are used and thus protected areas don't exist for the organization.

2. Access control to systems:

Accredible personnel are required to have a unique account to utilize systems in order to distinguish one user from another and establish accountability. Access to generic accounts is restricted to authorized individuals on an as needed basis through the use of a password management tool. A policy is in

place to ensure that Accredible personnel make use of the password management tool to produce and utilize secure passwords. Passwords are in place for all Accredible personnel on all platforms, where technically feasible or practical. Passwords must adhere to strict requirements which are documented in the Password Requirements and Guidelines document posted on the Intranet and referred to in theAccess Control Policy.

Administrator-level privileges for servers are restricted to authorized personnel who have been vetted and have the necessary experience to responsibly access resources.

Terminals and workstations are protected by time-out facilities which are activated after a time period of inactivity has elapsed.

Hard drives of mobile devices like notebooks etc. are encrypted. Encryption is enforced for any removable media like CD/DVD or USB mass storage devices. Mobile devices all require authentication to access and have remote-wipe enabled.

3. Access control to data:

All requests for application or system access, including remote (dial-up) access, are submitted through the IT Access Request Database. The functional manager, data owner, or other authorized approver must approve each request. Documentation is maintained.

Security Administration generates user access lists for in-scope applications, databases, and related UNIX and Windows servers with the associated access

rights for the designated business owners/IT managers. The business owners/IT managers are responsible for reviewing and approving these lists at least annually.

4. Disclosure Control:

All electronic data transfer among all workplaces and data centres makes use of the corporate VPN network which is encrypted.

To access the network for business reasons from external locations, business associates may use the corporate SSLVPN. To obtain access to VPN the user must complete a VPN ID request and use a corporate asset to access VPN which is configured with antivirus, antispyware and personal firewall software.

File transfers outside of the company consist of an encrypted package sent via email, regular FTP or by using SFTP. TLS is used for email with clients in situations where the client is able to use TLS also.

Backups are encrypted and transported over SSL to remote data centres.

5. Input Control:

Logging is enabled on applications, servers and databases. Some application systems produce transaction logging.

6. Job control:

Under the Accredible DPA, Personal Data are processed by Accredible only according to the Customer's instructions. Internally, the Accredible ensures by provisions in work contracts, guidelines and statements of work that the

Customer’s instructions are being met.

The Customer is entitled to inspect the Accredible’s adherence to its instructions as per the provisions of the Accredible DPA.

7. Availability Control:

The anti-spam gateway, email environment and individual desktop and servers all run anti-virus software. Virus signature files residing on both desktops and servers are updated automatically at least once per day. Programs and data files that are on the network and at risk of infection from viruses are scanned as they are accessed. Virus alerts are reviewed and appropriate actions are taken to resolve issues identified. Identified issues that require action are logged in a Service Desk ticket.

Data centres are backed up on a daily basis and supply redundancy where possible. Backup is performed according to the data backup policy and disaster recovery plan is in place and tested as required.

8. Separation Control:

Systems and applications are processed in different independent environments (DEV/QA/PROD). This ensures the segregation of functions.

Access profiles (e.g. roles and security groups) are used for granting privileges whenever possible. Naming conventions for these roles and groups reflect privilege levels.

Appropriate segregation of duties shall be incorporated in access rights

management processes, e.g., Accredible users cannot change their own privileges or approve their own requests. The auditing and review of IDs to ensure compliance must be run on a scheduled basis.

Multi-user application systems are designed with security controls in an effort to ensure that:

- Appropriate authorization is required to access, modify, save or delete information;
- Secure or administrative functions are only displayed or documented to authorized IT users;
- System design and development includes appropriate controls to ensure security and prevent system compromise; and
- Application security controls are a supplement, not replacement, for available systems, database and operating system controls.

Security Administration is restricted to the Security Admin group.

9.Accredible Self-Audit:

Accredible will by itself regularly audit and assess compliance with the obligations set out in this Exhibit 1.

Exhibit 2– Accredible Data Transfer Impact Assessment Questionnaire

This Exhibit 2 forms part of the Accredible DPA. Capitalized terms not defined in this Exhibit 2 have the meaning set forth in the Accredible DPA.

1. What countries will Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored

in or accessed from? If this varies by region, please specify each country for each region.

1.a **Answer**: United States, United Kingdom.

2. What are the categories of Data Subjects whose Personal Data will be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

2.a **Answer**: Customer's end users such as employees, students or other Data Subjects for which Customer wants to create certificates/accreditations.

3. What are the categories of Personal Data transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

3.a **Answer**: Personal Data that is Processed in connection with the Services including, but not limited to, name, email, location, information on individual performance for which a certificate/accreditation will be granted.

4. Will any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom? If so, are there any 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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures?

4.a **Answer**: Not to Accredible's knowledge.

5. What business sector is Accredible involved in?

5. a **Answer**: Cloud software.

6. Broadly speaking, what are the services to be provided and the corresponding purposes for which Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

6.a **Answer**: Accredible is a software company that offers client cloud based services for the design, issuance, administration and monitoring of digital certificates and badges using Accredible's online platform. Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom in order to the provide the Services.

7. What is the frequency of the transfer of Personal Data outside of outside of the European Economic Area, Switzerland, and/or the United Kingdom? E.g., is Personal Data transferred on a one-off or continuous basis?

7.a **Answer**: Personal Data is transferred on a continuous basis as a result of Customer's use of the Services.

8. When Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom to Accredible, how is it transmitted to Accredible? Is the Personal Data in plain text, pseudonymized, and/or encrypted?

8.a **Answer**: Accredible uses industry-standard Transport Layer Security ("TLS") to create a secure connection using 128-bit Advanced Encryption Standard ("AES") encryption. This includes all Personal Data sent between the web

properties apps and the Accredible servers. All connections are made securely over HTTPS.

9. What is the period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period?

9.a **Answer**: Personal Data will be retained in accordance with the Accredible DPA.

10. Please list the Subprocessors that will have access to Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom:

10.a **Answer**: As set forth in Section 6.4 of the Accredible DPA.

11. Is Accredible subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where Personal Data is stored or accessed from that would interfere with Accredible fulfilling its obligations under the attached Standard Contractual Clauses? For example, FISA 702 or U.S. Executive Order 12333. If yes, please list these laws.

11.a **Answer**: As of the effective date of the Cloud Services Agreement, no court has found Accredible to be eligible to receive process issued under the laws contemplated by Question 11, including FISA Section 702 and no such court action is pending.

12. Has Accredible ever received a request from public authorities for information pursuant to the laws contemplated by Question 11 above (if any)? If yes, please explain.

12.a **Answer**: As of the effective date of the Cloud Services Agreement, Accredible has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the CJEU Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, nor is Accredible aware of any such orders in progress.

13. Has Accredible ever received a request from public authorities for Personal Data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.

13.a **Answer**: No.

14. What safeguards will Accredible apply during transmission and to the processing of Personal Data in countries outside of the European Economic Area, Switzerland, and/or the United Kingdom that have not been found to provide an adequate level of protection under Applicable Laws?

14.a **Answer**: As set forth in Exhibit 1.

Exhibit 3 – Standard Contractual Clauses

This Exhibit 3 forms part of the Accredible DPA.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

(e) To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include

the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.

(e) To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties processing of personal data that is subject to the United Kingdom General Data Protection Regulation as supplemented by terms in the Data Protection Act 2018.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause – Omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate

technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide

the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or

practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of

confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far 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, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data
importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin,

political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations

to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these

Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) Where the data exporter is established in an EU Member State, the following section applies: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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 following section applies: 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, as indicated in Annex I.C, shall act as competent supervisory authority.

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, the following section applies: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act

as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to

the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

1. Name: Customer.

Address: As set forth in the Notices section of the Cloud Services Agreement.

Contact person's name, position and contact details: As set forth in the Notices section of the Cloud Services Agreement.

Activities relevant to the data transferred under these Clauses: As set forth in Exhibit 2.

Role (controller/processor): Controller.

Data importer(s):

1. Name: Accredible.

Address: As set forth in the Notices section of the Cloud Services Agreement.

Contact person's name, position and contact details: As set forth in the Notices section of the Cloud Services Agreement.

Activities relevant to the data transferred under these Clauses: As set forth in Exhibit 2.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

As set forth in Exhibit 2.

Categories of personal data transferred

As set forth in Exhibit 2.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As set forth in Exhibit 2.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

As set forth in Exhibit 2.

Nature of the processing

As set forth in Exhibit 2.

Purpose(s) of the data transfer and further processing

As set forth in Exhibit 2.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As set forth in Exhibit 2.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
As set forth in Exhibit 2.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

ANNEX II

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

MODULE TWO: Transfer controller to processor

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer shall implement and maintain appropriate technical and organisational measures designed to protect personal data in accordance with the Accredible DPA.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the Accredible DPA.

ANNEX III

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

UK Addendum to the EU Commission Standard Contractual Clauses

Date of this Addendum:

1. The Clauses are dated as of the same date as the Accredible DPA.

Background:

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data 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. This Addendum forms part of and supplements the Clauses to which it is attached. If Personal Data originating in the United Kingdom is transferred by Customer to Accredible in a country that has not been found to provide an adequate level of protection under UK Data Protection Laws, the Parties agree that the transfer shall be governed by the Clauses as supplemented by this Addendum.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Annex those terms shall have the same meaning as in the Annex. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
The Annex	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

UK GDPR	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.
UK	The United Kingdom of Great Britain and Northern Ireland

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 UK GDPR.

5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

7. In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

8. This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:

a. for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and

b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

9. The amendments required by Section 8 above, include (without limitation):

a. References to the "Clauses" means this Addendum as it incorporates the Clauses

b. Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data 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."

c. 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.

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

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

f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;

g. Clause 17 is replaced to state “These Clauses are governed by the laws of England and Wales”.

h. Clause 18 is replaced to state:

“Any dispute arising from these Clauses 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”.

i. The footnotes to the Clauses do not form part of the Addendum.