PINGBOARD DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) is between Pingboard, Inc., a Delaware corporation (“**Pingboard**”) and the customer specified in the table below (“**Customer**”). Customer and Pingboard may be referred to individually as a “Party” and collectively as the “Parties”.

Pingboard, Inc. By: ______________________________ Name: ___________________________ Title: ____________________________ Signature Date: __________________ Address: 21750 Hardy Oak Blvd, Suite 104, PMB 46048, San Antonio, TX 78258-4946 USA Data Protection Officer’s email address: dpo@pingboard.com	**Customer:** ____ (full legal entity name) By (signature): _________________________________ Your Printed Name: _____________________________ Your Title: _______________________________________ Signature Date: __________________________________ Customer Address: ____ ____ ____ Email Address(es) for notifications related to this DPA, including the of appointment of new Sub-processors: ____ ____ ____

This DPA forms part of the master services agreement, terms of service or other agreement, as applicable (the “**Agreement**”), between Customer and Pingboard, pursuant to which Customer has purchased subscriptions to Pingboard’s services (“**Services**”) and is applicable to Personal Data to the extent it is covered by Applicable Data Protection Laws and Processed by Pingboard in connection with the Services.

The parties agree to comply with the following provisions, each acting reasonably and in good faith.

1. Definitions

For purposes of this DPA, the following terms have the meaning stated:

"**CCPA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act ("**CPRA**"), and its accompanying regulations, each as they may be amended from time to time.

"**CPA**" means the Colorado Privacy Act and its accompanying regulations, each as they may be amended from time to time.

"**Controller**" means the entity that determines the purposes and means of the Processing of Personal Data, which includes a 'business' as that term is defined in the CCPA.

"**CTDPA**" means the Connecticut Data Privacy Act and its accompanying regulations, each as they may be amended from time to time.

"Data Protection Laws" means any laws and regulations applicable in any relevant jurisdiction relating to privacy or the use or processing of data relating to natural persons, including without limitation: (a) any state or federal laws or regulations in the United States including without limitation the CCPA, VCDPA, CPA, UCPA and CTDPA; (b) GDPR; (c) UK GDPR; (d) the DPA 2018; (e) EU Directive 2002/58/EC (as amended by 2009/139/EC) and any legislation implementing or made pursuant to such directive, including (in the UK) the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (f) any laws or regulations ratifying, implementing, adopting, supplementing or replacing GDPR, UK GDPR and/or the DPA 2018; in each case, to the extent in force, and as such are updated, amended or replaced from time to time.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates and includes a 'consumer' as that term is defined in the CCPA.

"**EEA**" means the European Economic Area, including Switzerland and those countries comprising the European Union ("EU") and the European Free Trade Association.

"EU SCCs" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data in countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).

"**GDPR**" means: (i) the EU General Data Protection Regulation (2016/679) and any implementing laws in each EU member state as they may be amended from time to time, and (ii) the United Kingdom's Data Protection Act 2018 and any implementing laws in the United Kingdom as they may be amended from time to time.

"**Personal Data**" means all data which is defined as 'personal data' or 'personal information' in the Applicable Data Protection Laws, and which is provided by Subscriber to Pingboard or accessed, stored or otherwise processed by Pingboard in connection with the Services.

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

"**Processor**" means the entity that Processes Personal Data on behalf of the Controller, and includes a 'service provider' as that term is defined in the CCPA.

"**Security Incident**" means a breach of Pingboard security or a Pingboard Sub-processor's security leading to accidental or unlawful destruction, theft, loss, alteration, unauthorised disclosure of, or access to Personal Data.

"**Subscriber**" means Customer and any corporate entities which from time to time: (a) directly or indirectly control, are controlled by, or are under common control with the Customer; and (b) for purposes of GDPR are established and/or doing business in the United Kingdom and/or the European Economic Area or Switzerland, and for purposes of CCPA share common branding with Customer. "Control," for purposes of this definition, means direct or indirect ownership of, power to vote, or other control of more than 50% of the voting interests of the subject entity, control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. “Common branding” means a shred name, service mark, or trademark.

“**Supervisory authority**" shall have the meanings ascribed to it in the GDPR.

"UK GDPR" means the GDPR 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 in the UK.

“**UK Addendum**” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the United Kingdom’s Information Commissioner’s Office and in force as of March 21, 2022 and attached as Schedule 2 hereto.

“**UCPA**” means the Utah Consumer Privacy Act and its accompanying regulations, each as they may be amended from time to time.

“**VCDPA**” means the Virginia Consumer Data Protection Act and its accompanying regulations, each as they may be amended from time to time.

Capitalized terms used, but not defined, in this DPA are defined in the Agreement.

2. Processing of Personal Data

The parties acknowledge and agree that with regard to the Processing of Personal Data, Subscriber is the Controller, and Pingboard is the Processor.

Pingboard shall only Process Personal Data as follows: (i) on behalf of and in accordance with Subscriber’s documented instructions for the following purposes: (A) Processing in accordance with the Agreement; (B) Processing initiated by Users in their use of the Services; and (C) Processing to comply with other documented reasonable instructions provided by Subscriber (e.g. via contacting Pingboard's customer support) where such instructions are consistent with the terms of the Agreement, and (ii) as required by Applicable Data Protection Laws.

Subscriber’s instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws. Subscriber shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Subscriber acquired Personal Data, including compliance with any applicable Data Subject notice and consent requirements.

For clarity, Pingboard shall not sell Subscriber’s Personal Data as the term ‘sell’ is defined in the CCPA.

Details of the Processing of Personal Data.

(a) The subject matter of Processing of Personal Data by Pingboard is the performance of the Services pursuant to the Agreement.

(b) The duration of the Processing is the Term, as defined in the Agreement, and any period after Term prior to Pingboard's deletion of the Personal Data (“Duration of Processing”).

(c) The nature and purpose of the Processing is to enable Subscriber to receive and Pingboard to provide the Services pursuant to the Agreement and as further instructed by Subscriber in its use of the Services.

(d) Subscriber may submit Personal Data to the Services, the extent of which is determined and controlled by Subscriber in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: name, job title, employer, contact information, ID data, professional life data, personal life data, localization data, images, and other content or data in electronic form stored or transmitted by Subscriber and its Users via the Services.

(e) To the extent Subscriber submits Personal Data to the Services, it may concern Subscriber's employees, owners, investors, vendors, partners, consultants, customers, prospects, agents, advisors, Users and other contacts of the Subscriber.

3. Personnel

Pingboard shall take reasonable steps to ensure the reliability of any employee, agent or contractor engaged by Pingboard in the Processing of Personal Data, ensuring that access is strictly limited to those individuals who need access as necessary for the purpose of the Agreement and DPA and to comply with Applicable Data Protection Laws, ensuring that all such individuals are informed of the confidential nature of the Personal Data, have executed written confidentiality agreements, and that such confidentiality obligations survive the termination of the personnel engagement.

4. Security

Pingboard shall maintain technical and organizational measures appropriate (having regard to the state of technological development and cost of implementation) for protection of the security, confidentiality and integrity of Personal Data (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss, theft or alteration or damage, unauthorized disclosure of, or access to, Personal Data), as set forth in the Pingboard Security Brief published at https://pingboard.com/security ("Security Measures"). Pingboard regularly monitors compliance with the Security Measures and Pingboard will not materially decrease the overall security of the Services during the Duration of Processing. Subscriber agrees that the Security Measures are appropriate for the categories of Personal Data being Processed.

5. Sub-Processing

Subscriber acknowledges and agrees that Pingboard may appoint third-parties to assist in providing the Services and processing of Personal Data ("**Sub-processors**"), provided that such Sub-processors:

(a) agree to act only on Pingboard's instructions when processing Personal Data (which instructions shall be consistent with the Subscriber's processing instructions to Pingboard); and

(b) have entered into a written agreement with Pingboard containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Sub-processor

Pingboard shall make available to Subscriber the current list of Sub-processors used for the processing of Personal Data under this DPA at https://pingboard.com/legal/subprocessors. When any new Sub-processor is appointed that will Process Personal Data, Pingboard will, at least thirty (30) days before the new Sub-processor processes any Personal Data, notify Subscriber of the appointment via email at the email address(es) listed in the signature block of this DPA.

In the event that Subscriber reasonably objects to the processing of its Personal Data by any Sub-processor, it shall inform Pingboard immediately by emailing its objection and the grounds for its objection to dpa@pingboard.com. In such event, Pingboard will do one of the following at Pingboard's option: (a) instruct the Sub-processor to cease any further processing of the Subscriber's Personal Data, in which event this DPA shall continue unaffected, or (b) allow the Subscriber to terminate this DPA and the Agreement and related Services immediately, in which case Pingboard will provide Subscriber with a pro rata refund of any payment paid in advance for Services but not yet received by Subscriber.

Pingboard shall be liable for the acts and omissions of its Sub-processors to the same extent Pingboard would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

The Service provides links to integrations with third-party services, which Customer may, at Customer's sole discretion, integrate directly into Customer's instance of the Service and may have access to, or process, Subscriber's Personal Data. The providers of these third-party services shall not be deemed Sub-processors for any purpose under this DPA. If Customer elects to enable, access or use such third-party services, its access and use of such third-party services is governed solely by the terms and conditions and privacy policies of such third-party services, and Pingboard does not endorse, is not responsible or liable for, and makes no representations as to any aspect of such third-party services, including, without limitation, the manner in which they handle Subscriber's Personal Data. Pingboard is not liable for any damage or loss caused or alleged to be caused by or in connection with Customer's enablement, access or use of any such third-party services, or Subscriber's reliance on the privacy practices, data security processes or other policies of such third-party services.

6. Data Transfers

The parties hereby agree that the EU SCCs attached at Schedule 1 will apply to the transfer of Personal Data, to the extent such transfers are subject to the GDPR and are to a country that the relevant regulatory authorities in the EEA or Switzerland, as applicable, do not recognize as providing an adequate level of protection for Personal Data (as described in the GDPR, and (ii) are not covered by a suitable alternative framework deemed by relevant authorities as providing an adequate level of protection of Personal Data. Pingboard may terminate the EU SCCs by giving Subscriber 30 days' notice on implementing an alternative framework as provided in the prior sentence.

The parties hereby agree that the UK Addendum attached at Schedule 2 will apply to the transfer of Personal Data from the United Kingdom, to the extent such transfers are subject to the GDPR and are to a country that the relevant regulatory authorities in the United Kingdom do not recognize as providing an adequate level of protection for Personal Data (as described in the GDPR, and (ii) are not covered by a suitable alternative framework deemed by relevant authorities as providing an adequate level of protection of Personal Data. Pingboard may terminate the UK Addendum by giving Subscriber 30 days' notice on implementing an alternative framework as provided in the prior sentence.

7. Rights of Data Subjects

Pingboard shall respond to any Data Subject complaint, inquiry, or request to exercise their rights regarding Personal Data (including right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making), ("**Data Subject Request**") by either asking the Data Subject to make their request to Subscriber or by promptly notifying the Subscriber of the same.

Pingboard will, in a manner consistent with the functionality of the Services, enable Subscriber to access, rectify, erase and restrict processing of Personal Data (including via the deletion functionality provided by the Service), and to export Personal Data.

To the extent Subscriber, in its use of the Services, does not have the ability to address a Data Subject Request, Pingboard shall upon Subscriber's request (and taking into account the nature of the Processing) provide commercially reasonable efforts to assist Subscriber in fulfilling its obligation to respond to Data Subject Requests that are required under Applicable Data Protection Laws. To the extent legally permitted, Subscriber shall be responsible for any reasonable costs arising from Pingboard's provision of such assistance.

8. California Consumer Privacy Act

Customer and Pingboard shall comply with the CCPA to the extent that the Customer is a Business and Pingboard is a Service Provider processing the Personal Data of Consumers on behalf of the Customer. It shall be the responsibility of Customer to inform Pingboard which Personal Data Pingboard Processes on behalf of the Customer is within the scope of the CCPA.

Customer warrants that it discloses Personal Data of Consumers to Pingboard solely for (i) a valid business purpose, and (ii) to permit Pingboard to perform the Services.

To the extent the CCPA is applicable, Pingboard shall not retain, use, or disclose Personal Data of Consumers obtained in the court of providing Services except:

- To process or maintain Personal Data of Consumers on behalf of the Customer in compliance with the Agreement;
- To retain and employ another Service Provider as a Sub-Processor, where the Sub-Processor meets the requirements for a Service Provider under CCPA;
- For internal use by Pingboard to build or improve the quality of its services, provided that the use does not including building or modifying Consumer profiles to use in providing Services to another Business or correcting or augmenting data acquired from another source; and/or
- To detect data Security Incidents, or to protect against fraudulent or illegal activity.

This DPA shall not restrict Pingboard’s ability to:

- Comply with federal, state, or local laws;
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena or summons by federal, state, or local authorities;
- Cooperate with law enforcement agencies concerning conduct or activity that the Customer, Pingboard, or a third party reasonably and in good faith believes may violate federal, state, or local law; and/or
- Exercise or defend legal claims.

For clarity, Pingboard shall not sell or share a Consumer’s Personal Data as the term ‘sell’ and “share” are defined in the CCPA when a Consumer has opted-out of the sale or sharing of their Personal Data with the Customer and such request has been conveyed to Pingboard.

9. Audit Rights

Upon Subscriber's request with not less than thirty (30) days' notice, Pingboard agrees (at Subscriber's expense) to permit Subscriber to perform reviews of Pingboard's compliance with its security obligations set forth under the DPA (the "**Subscriber Audits**"). Subscriber Audits may be conducted by the internal and external auditors and personnel of Subscriber who have entered into Pingboard's form of nondisclosure agreement (collectively, "**Auditors**"). Such Subscriber Audits shall be conducted in accordance with Pingboard's security policies and procedures, without undue disruption to Pingboard’s operations, in a commercially reasonable manner, and shall be limited to the security aspects of the Services provided to Subscriber. Pingboard agrees to cooperate in a commercially reasonable manner with the Auditors and provide the Auditors commercially reasonable assistance as they may reasonably request in connection with the Subscriber Audit. Except in the case of an audit performed in response to a Security Incident, Subscriber Audit(s) will be performed at Subscriber's sole cost and Subscriber will reimburse Pingboard for its reasonable costs associated with such additional Subscriber Audits. Pingboard shall bear all costs of audits performed in response to a Security Incident. Subscriber shall promptly notify Pingboard with information regarding the results of Subscriber Audits, including any information that Pingboard is not Processing Personal Data in accordance with its obligations under this DPA.

10. Data Protection Impact Assessment

Pingboard shall, taking into account the nature of the processing and the information available to Pingboard, provide reasonable assistance to Subscriber at Subscriber's cost, with any data protection impact assessments and prior consultations with supervisory authorities or other competent regulatory authorities as required for the Subscriber to fulfill its obligations under the GDPR or other applicable Data Protection Laws.

11. Security Incidents

Pingboard shall notify Subscriber without undue delay after becoming aware of a confirmed Security Incident, and provide reasonable information (the extent that such information is known or available to Pingboard) and cooperation to Subscriber so that Subscriber can fulfill any data breach reporting obligations it may have under Applicable Data Protection Laws. Pingboard shall take the steps as Pingboard deems necessary and reasonable in order to remedy or mitigate the effects of the Security Incident. The obligations herein shall not apply to incidents that are caused by Subscriber or Subscriber's Users.

12. Deletion of Personal Data

Pingboard shall enable Subscriber to retrieve and/or delete Personal Data from the Service before any termination of the Agreement. Subscriber instructs Pingboard, after the end of the provision of the Services, to delete all Personal Data in Pingboard's possession or control, and Pingboard shall delete such Personal Data within 90 days or shorter as required by Applicable Data Protection Laws, including, without limitation, when a Data Subject exercises their right to erasure, but this requirement shall not apply to the extent Pingboard is required by applicable law to retain all or some of the Personal Data or to Personal Data Pingboard has archived on backup systems, which data Pingboard shall securely isolate and protect from further processing expect to the extent required by such law, until such time as the relevant backup archive is destroyed in accordance with Pingboard's standard backup destruction policies, which shall not exceed 90 days after the date such data was backed up.

13. Subscriber Instructions

Pingboard shall not be liable for any claim brought by Subscriber or any third party arising from Pingboard's compliance with Subscriber's instructions.

14. General

13.1 This DPA sets out all of the terms that have been agreed between the parties in relation to the subjects covered by it.

To the extent that any provision of this DPA conflicts with any provision of the Agreement, the terms of the DPA shall, as to the specific subject matter of the DPA, take precedence over the conflicting provision in the Agreement.

13.2 This DPA shall remain in place until the earlier of:

(a) The expiry or termination of the Agreement (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination); or

(b) The parties agreeing in writing that this DPA is to be terminated.

The parties agree that, save as provided above, nothing in this DPA shall affect the application of the governing law section of the Agreement.

13.3 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

Schedule 1**: EU 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)[1] 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.

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.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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.

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 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[2] (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

(a) GENERAL WRITTEN AUTHORISATION 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

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

to that list through the addition or replacement of sub- processors at least 30 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.[3] 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

(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

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

subject.

OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[4] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(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

(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

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

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

(a) 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

(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[5];

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this

(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). [For Module Three: The data exporter shall forward the notification to the controller.]

(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 [for Module Three: , if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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

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

information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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.

[For Module Three: The data exporter shall forward the notification to the controller.]

(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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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.

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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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 [for Module Three: and the controller] 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

These Clauses shall be governed by the law of the country set forth in the Agreement, or if such law does not allow for third-party beneficiary rights, then the law of the EU Member State(s) of the data exporter or in which the majority of data subjects reside.

Clause 18 - Choice of forum and jurisdiction

(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 the Member State of the data exporter.

(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.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
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	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. 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

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data 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 data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "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";

c. 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.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with:

> “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

> “These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

> “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.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

15. Annex 1/Appendix 1 to the EU SCCs and UK Addendum

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

ANNEX I

A. List of Parties

Data exporter

The data exporter is: a Subscriber with data subjects in the European Economic Area who transfer Personal Data to Pingboard, Inc.

Data importer

The data importer is: Pingboard, Inc.

Description of Transfer

The Nature and Duration of the Processing are set forth in the Agreement. **Data subjects**

The Personal Data transferred concern the following categories of data subjects:

- The UK and EEA based employees, owners, investors, vendors, partners, consultants, customers, prospects, agents, advisors, Users and other contacts of the Data Exporter who use the Pingboard Services.

Categories of data

The Personal Data transferred concern the following categories of data:

- Personal information such as name, job title, employer, contact information, ID data, IP address, professional life data, personal life data, localization data, images, and other content or data in electronic form stored or transmitted via the Services.
- End user usage information of the Services, including information related to devices, browsers, and information about how the Services are accessed.

Subscriber agrees not to upload to the Service any personal data defined by the GDPR as “special categories” including data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation, health data, trade union membership, genetic data or biometric data.

Processing operations

The objective of Processing of Personal Data by the data importer is the performance of the services pursuant to the Agreement in place between the data exporter and the data importer.

B. Competent Supervisory Authority

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, shall act as competent supervisory authority

16. Annex 2/Appendix 2 to the EU SCCs and UK Addendum

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in Paragraph 4 of the DPA and in the Pingboard Security Documentation accessible via https://pingboard.com/security and at a minimum shall include the controls listed below. Data Importer will not materially decrease the overall security of the Services during the term of the Agreement.

1. **Data Access Control:** Access is granted on a least privilege, need-to-have and must-know basis to prevent disclosure. Users and their activities are uniquely identifiable and segregated by role. Administrative privileges are restricted to only those who need them.

2. **Information System Access Control:** Access is strictly controlled by a formal provisioning process. Information systems are password protected and have an owner responsible for managing and controlling access.

3. **Multi-factor Authentication:** Data importer personnel are only granted access to personal data and critical technology after successfully presenting multiple, separate pieces of evidence.

4. **Physical Access Control:** Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where personal data and critical technology are located.

5. **Transmission Control:** All personal data transmitted through a public network (e.g., the internet) must be encrypted or sent via a secure channel.

6. **Separation Control:** Network services, systems, workstations, and servers are separated based on business purpose.

7. **Availability Control:** To protect against loss of data, information systems are subject to backup and built-in redundancy.

8. **Patch Management Control:** System patches are implemented in a reasonable, risk-based timeframe.

9. **Security Awareness Training:** Persons who may have access to personal data or critical systems are trained annually on topics related to the importance of information security and safeguards against data loss, misuse or breach through physical, logical and social engineering mechanisms.

17. Annex 3 to the EU SCCs: List of Sub-processors

See Section 5 of DPA.

https://pingboard.com/legal/subprocessors