Data Processing Addendum

This Data Processing Addendum is effective as of the date you agreed to the Terms.

PARTIES

Under the terms of this DPA, Customer shall be the Controller and Sandhills shall be the Processor of the Personal Data.

RECITALS

WHEREAS, the Customer and Sandhills entered into the Terms that require Sandhills to Process Personal Data provided by or collected for the Customer; and

WHEREAS, this Data Processing Addendum sets out the additional terms, requirements, and conditions on which Sandhills will Process Personal Data when providing services under the Terms;

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereto agree as follows:

1) Definitions and Interpretation.
   a) The following definitions and rules of interpretation apply in this DPA.
      i) "Business Purpose" means the services described in the Terms or any other purpose specifically identified in Exhibit 1.
      ii) “Controller” shall have the meaning given to it by Privacy and Data Protection Requirements, or any analogous term used to denote the Party which determines the purposes and means of the Processing of the Personal Data. For example, the term Business under the CCPA/CPRA.
      iii) "Data Subject" means an individual who is the subject of the Personal Data and to whom or about whom the Personal Data relates or identifies, directly or indirectly.
      iv) “DPA” means this Data Processing Addendum.
      v) “EU SCCs" means the European Commission's standard contractual clauses for the transfer of personal data from the European Union to third countries approved by the European Commission in decision 2021/914, as described below in Exhibit 2.
      vi) “FADP” means the Swiss Federal Act on Data Protection of 25 September 2023, as may be amended, superseded, or replaced.
      vii) “GDPR” means the General Data Protection Regulation (EU/2016/679) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding

the processing of personal data and on the free movement of such data, as may be amended, superseded, or replaced.

viii) "Privacy and Data Protection Requirements" means all applicable federal, state, and foreign laws and regulations relating to the processing, protection, or privacy of Personal Data, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. This includes, but is not limited to, the General Data Protection Regulation, California Consumer Privacy Act, Virginia Consumer Data Protection Act, etc.

ix) “Processor” shall have the meaning given to it by Privacy and Data Protection Requirements, or any analogous term used to denote the Party which Processes Personal Data on behalf of the Controller. For example, the term Service Provider under the CPRA.

x) "Processing, Processes, or Process" means any activity that involves the use of Personal Data or that the relevant Privacy and Data Protection Requirements may otherwise include in the definition of processing, processes, or process. It includes obtaining, recording, holding the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Data to third parties.

xi) "Security Breach" means any act or omission that compromises the security, confidentiality, or integrity of Personal Data or the physical, technical, administrative, or organizational safeguards put in place to protect it. The loss of or unauthorized access, disclosure, or acquisition of Personal Data is a Security Breach whether or not the incident rises to the level of a security breach under the Privacy and Data Protection Requirements.

xii) “Share” or “Shared” or “Sharing” means disclosing, making available, transferring, or otherwise communicating Personal Data to a third party for cross-context behavioral advertising / targeted advertising, as those terms are defined under Privacy and Data Protection Requirements, whether or not for monetary or other valuable consideration.

xiii) “Sell” or “Sale” or “Sold” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject’s Personal Data to a third party for monetary or other valuable consideration.

xiv) "Subprocessor" means any third party appointed by the Processor to assist in fulfilling its obligations in providing services to the Controller.

xv) “UK Addendum” means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner, Version B1.0 in force as of March 21, 2022.

xvi)"UK GDPR" means the United Kingdom General Data Protection Regulation, being the GDPR as it forms part of the domestic law of the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419)), read together with the Data Protection Act 2018, as may be amended, superseded, or replaced.

b) This DPA is subject to and incorporated into the Terms. Interpretations and defined terms set forth in the Terms apply to the interpretation of this DPA, unless otherwise defined in this DPA.

c) The Exhibits form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Exhibits.

d) A reference to writing or written includes via email or mail.

e) In the case of conflict or ambiguity between:

i) Any provisions contained in the body of this DPA and any provisions contained in the Exhibits, the provisions in the body of this DPA will prevail;

ii) Any of the provisions of this DPA and the provisions of the Terms, the provisions of this DPA will prevail; and

iii) Any of the provisions of this DPA and any EU SCCs, the provisions of the EU SCCs will prevail.

2) Personal Data Types and Processing Purposes.

a) The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Privacy and Data Protection Requirements, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Sandhills as its Processor.

b) Customer is disclosing the Personal Data to Sandhills only for the limited and specific Business Purposes set forth within this DPA.

c) Exhibit 1 describes the general Personal Data categories, nature and purpose of processing, and other information regarding the Processing that Sandhills will undertake to fulfill the Business Purposes of the Terms.

3) Sandhills Obligations.

a) Sandhills will only Process, retain, use, or disclose the Personal Data to the extent, and in such a manner, as is necessary for the Business Purpose(s) and in accordance with the Customer's written instructions.

b) Sandhills will not Process, retain, use, or disclose the Personal Data that it collects or receives for any other purpose, outside of the Parties' business relationship, or in a way that does not comply

with this DPA or the Privacy and Data Protection Requirements, unless expressly permitted by Privacy and Data Protection Requirements. This includes combining or updating the Personal Data with Personal Data that Sandhills received from another source or collected from its own interaction with a Data Subject, unless the Privacy and Data Protection Requirements permit the action.

c) Sandhills must promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with this DPA and/or Privacy and Data Protection Requirements.

d) Sandhills will not retain, use, or disclose the Personal Data that it Processes under this DPA for any purpose other than the Business Purposes(s) specified within this DPA, unless expressly permitted by Privacy and Data Protection Requirements.

e) Upon notice from Customer, Sandhills shall promptly comply with any reasonable and appropriate requests or instructions from Customer requiring Sandhills to amend, transfer, or delete the Personal Data, or to stop, mitigate, or remedy any unauthorized Processing or Processing that Customer believes is not in compliance with Privacy and Data Protection Requirements.

f) Sandhills will ensure that the Personal Data is not Sold or Shared and will not disclose Personal Data to third parties unless the Customer or this DPA specifically authorizes the disclosure, or as allowed by law. If a law requires Sandhills to disclose Personal Data, Sandhills must first inform the Customer of the legal requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

g) Sandhills will reasonably assist Customer with meeting Customer's compliance obligations under the Privacy and Data Protection Requirements, taking into account the nature of the Sandhills' Processing and the information available to Sandhills. This includes but is not limited to, assisting in responding to regulatory inquiries, assisting with prior consultations with supervisory authorities, assisting in data subject access request, assisting in completing data protection or security assessments, or assisting in other similar privacy reviews of Customer's Processing activities, and providing documentation or answering inquiries from Customer in the furtherance of meeting Customer's obligations under Privacy and Data Protection Requirements.

h) Sandhills shall promptly notify Customer of any changes in its ability to meet current or future requirements under Privacy and Data Protection Requirements.

i) Sandhills shall comply with all Privacy and Data Protection Requirements, including with respect to Personal Data that it Processes pursuant to this DPA, and provide the same level of privacy protection as required by Customer under Privacy and Data Protection Requirements.

j) Sandhills shall ensure that it and anyone operating on its behalf will Process the Personal Data in compliance with this DPA and all applicable Privacy and Data Protection Requirements and other laws, enactments, regulations, orders, standards, and other similar instruments.

k) Sandhills represents that it has no reason to believe that any Privacy and Data Protection Requirements prevent it from providing any of the Term's contracted services.

4) Confidentiality.

a) Sandhills will ensure that all personnel who are engaged in the Processing of Customer's Personal Data:

i) are informed of the Personal Data's confidential nature and are subject to written confidentiality agreements or statutory confidentiality obligations; and

ii) are aware of both Sandhills' duties and their personal duties and obligations under the Privacy and Data Protection Requirements and this DPA.

5) Security

a) Sandhills shall at all times implement appropriate technical and organizational measures designed to safeguard Personal Data against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, destruction, unavailability, or damage including, but not limited to, the security measures set out in Exhibit 4 and any additional security measures required by Privacy and Data Protection Requirements. The security measure taken shall ensure a level of security appropriate to 1) the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction, or damage; 2) the nature of the Personal Data protected; and 3) comply with all Privacy and Data Protection Requirement. Sandhills shall document those measures in writing and periodically review them, at least annually, to ensure they remain current and complete.

b) Sandhills shall take reasonable precautions to preserve the integrity of any Personal Data it Processes and to prevent any corruption or loss of the Personal Data, including but not limited to establishing effective back-up and data restoration procedures.

6) Security Breaches and Personal Data Loss.

a) Sandhills shall notify Customer without undue delay after becoming aware of a Security Breach.

b) Sandhills will not inform any third party of a Security Breach without first obtaining the Customer's prior written consent, except when law or regulation requires Sandhills to inform a third party.

c) Notwithstanding clause 6(b), Sandhills agrees that Customer has the right to determine:

i) whether to provide notice of the Security Breach to any Data Subjects, regulators, law enforcement agencies, or others, as required by law or regulation or in Customer's discretion, including the contents and delivery method of the notice; and

ii) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

d) Immediately following the detection of a Security Breach, the Parties will coordinate with each other to investigate the matter. Additionally, Sandhills will reasonably cooperate with Customer in the Customer's handling of the matter.

e) Notification or information provided under this Clause shall not be interpreted or construed as an admission of fault or liability by Sandhills.

f) Customer shall be responsible for all reasonable costs and expenses associated with the performance of the obligations in this Clause 6.

7) Cross-Borders Transfer of Personal Data.

a) Where the Privacy and Data Protection Requirements restrict cross-border transfers of Personal Data and an appropriate transfer mechanism is required, Customer shall transfer Personal Data to Sandhills only where one or more of the following conditions is satisfied:

i) Sandhills, either through its location or participation in a valid cross-border transfer mechanism under the Privacy and Data Protection Requirements, may legally receive that Personal Data, however Sandhills must immediately inform Customer of any change to that status; or

ii) if any Personal Data transfer between Sandhills and Customer requires execution of standard contractual clauses in order to comply with the Privacy and Data Protection Requirements, the Parties agree that: (A) with respect to transfers subject to the GDPR, the EU SCCs contained in Exhibit 2 shall govern the transfer; and (B) with respect to transfers subject to the UK GDPR, the UK Addendum contained in Exhibit 3 shall apply to the EU SCCs as set out in Exhibit 2, and in each case, the Parties shall take all other actions required to legitimize the transfer, including implementing any needed supplementary measures or supervisory authority consultations; or

iii) the transfer otherwise complies with the Privacy and Data Protection Requirements.

b) Sandhills shall not transfer any Personal Data to a country outside the country from which it was originally transferred unless the transfer is made pursuant to a valid transfer mechanism under the Privacy and Data Protection Requirements, including, as applicable, the EU SCCs (Exhibit 2), the

UK Addendum (Exhibit 3), or the FADP modifications set out in Clause 7(c), or is otherwise in compliance with the Privacy and Data Protection Requirements.

c) Where Customer's Personal Data is protected by the FADP and is subject to a restricted transfer to a country that does not ensure an adequate level of data protection within the meaning of Article 16(1) of the FADP, the EU SCCs shall apply as set forth in Exhibit 2 with the following modifications:

(1) In Clause 13, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner;

(2) In Clause 17, the EU SCCs shall be governed by the laws of Switzerland;

(3) In Clause 18(b), disputes will be resolved before the courts of Switzerland;

(4) The term "Member State" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of bringing claims in their place of habitual residence (Switzerland) in accordance with Clause 18(c);

(5) All references to the GDPR or Regulation (EU) 2016/679 in the EU SCCs shall be interpreted as references to the FADP, and all references to the EU or EU Member States shall be interpreted to include Switzerland, in each case to the extent necessary to give effect to these modifications.

8) Subprocessors

a) In order to provide the services contemplated under the Terms, Sandhills will need to engage Subprocessors to assist with the Processing of Personal Data. Sandhills shall ensure that any Subprocessor it engages will comply with all Privacy and Data Protection Requirements in connection with the Processing of Personal Data pursuant to the Terms.

b) Sandhills shall enter into a written contract with the Subprocessor(s) that contains terms substantially the same as those set out in this DPA.

c) Sandhills shall remain liable to Customer for the actions and omissions of its Subprocessors if they fail to fulfill their respective data protection obligations with regard to the Processing under the Terms.

d) Sandhills shall list all currently approved Subprocessors in Exhibit 5, which includes their name, location, and a description of the Processing they will be undertaking. By entering into this DPA, Customer approves the use of the Subprocessors currently listed in Exhibit 5.

e) Sandhills may only add or replace Subprocessors if Customer is given 30 calendar days notice. Such notice shall contain the information in Clause 8(d). Sandhills shall provide notice of any

additions or replacements by sending an email to the primary contact associated with Customer's domain listed in Sandhills' systems. Customer may also view the current list of Subprocessors at the link in Exhibit 5. Any publication of an addition and/or replacement at the webpage in Exhibit 5 shall also be considered a notification to Customer.

f) Should Customer wish to object to the use of a particular Subprocessor, then Customer shall provide Sandhills with its written, good faith, reasonable objection to the use of the proposed Subprocessor within 15 calendars days of receiving notification or publication. If Customer does not object in a timely manner, Customer will be deemed to have consented to the use of the proposed Subprocessor.

g) Upon receiving a timely delivered opposition from Customer, Sandhills shall have the right to resolve the Customer's opposition through one of the following solutions, to be selected at Sandhills' sole discretion. Sandhills may: i) terminate or modify its plan to use the proposed Subprocessor; ii) take corrective measures to resolve the reasons for Customer's opposition to the use of the proposed Subprocessor and then continue with the use of the proposed Subprocessor; or iii) terminate the Terms.

9) Complaints, Data Subject Requests, and Third-Party Rights

a) Sandhills shall promptly notify Customer if it receives any complaint, notice, or communication from a governmental body or agency that relates to the Personal Data Processing under the Terms or either Party's compliance with its Privacy and Data Protection Requirements under this DPA.

b) Sandhills shall notify the Customer within three working days if it receives a request from a Data Subject to exercise any rights they may have regarding their Personal Data, such as access, correction, deletion, or to opt-out of or limit certain activities like sales, disclosures, or other Processing. Sandhills shall not respond to a data subject request itself unless it has been authorized by Customer or is required to do so under Privacy and Data Protections Requirements. However, Sandhills may inform the Data Subject that it is a Processor of Personal Data and that their request should be directed to Customer instead.

c) Sandhills shall give the Customer reasonable assistance in responding to or honoring any complaint, notice, communication, or effectuating any Data Subject request.

d) Should Customer receive a request from a Data Subject to exercise their privacy rights and Customer believes that Sandhills may need to take action on or assist with the request, then Customer shall send an email to privacyresponse@sandhills.com. The email shall contain enough information about the request and the Data Subject for Sandhills to be able to properly process the

request. Customer agrees to provide reasonable assistance to Sandhills to honor or respond to such requests.

10) Term and Termination

a) This DPA will remain in full force and effect so long as the Terms remain in effect.

b) Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Terms in order to protect Personal Data will remain in full force and effect.

c) Sandhills or Customers failure to comply with the terms of this DPA is a material breach of the Terms. In such event, the non-breaching Party may terminate the Terms or any part of the Terms authorizing the Processing of Personal Data pursuant to the Termination provisions of the Terms.

d) If a change in any Privacy and Data Protection Requirement or either Party's circumstances prevents a Party from fulfilling all or part of its obligations under the Terms, the Parties will suspend the Processing of Personal Data until the Parties Processing complies with applicable requirements. If the Parties are unable to bring the Personal Data Processing into compliance with the Privacy and Data Protection Requirements within 30 calendar days, they may mutually terminate the Terms.

11) Data Return and Destruction

a) Upon termination or expiration of the Terms, Sandhills shall securely delete, or at Customer's request return and not retain, within 60 calendar days all Personal Data related to the Terms in its possession or control. However, Sandhills reserves the right to retain backs ups because it may be embedded in its electronic and offsite files as part of its systematic back-up and archiving procedures.

b) Notwithstanding Clause 11(a), if any law, regulation, or government or regulatory body requires Sandhills to retain certain Personal Data that Sandhills would otherwise be required to return or destroy, it shall be allowed to retain the Personal Data for as long as Sandhills deems necessary. Sandhills may only use this retained Personal Data for the reason that requires such retention or for audit purposes.

12) Audits

a) Sandhills shall permit Customer, or an independent auditor agreed upon by the Parties, to conduct audits or inspections to ensure compliance with the terms of this DPA and/or Privacy and Data Protection Requirements. The scope of the audit shall be limited by the Parties to the systems, procedures, and documentation relevant to the Processing of Personal Data under the Terms. Sandhills agrees to provide Customer with all necessary cooperation, access, and support to conduct

such audits. The Parties shall consider the findings of any such audit confidential information subject to the Terms.

b) An audit conducted under Clause 12(a) may only be conducted:
   i) upon at least 30 calendar days' written notice and upon a date mutually agreed upon by both Parties;
   ii) during regular business hours of Sandhills and without significant interruption to Sandhills' business;
   iii) by auditors who have agreed to, or to whom apply, confidentiality requirements at least similar to the confidentiality requirements as applicable between Customer and Sandhills;
   iv) not more than once per 12 months, unless otherwise required by Privacy and Data Protection Requirements;

c) Notwithstanding Clause 12(a), Sandhills may instead arrange for a qualified and independent assessor to conduct an audit, at least annually, of Sandhills in support of the obligations contained in this DPA and/or Privacy and Data Protection Requirements using an appropriate and accepted control standard or framework and assessment procedure to conduct such audit. Upon Customer's request, Sandhills shall provide documentation or verification to show compliance with the control standard or framework and assessment procedure Sandhills has attained. Customer agrees to accept this documentation in lieu of requesting an audit under Clause 12(a).

d) Should the documentation provided under Clause 12(c) not address the controls necessary to demonstrate Sandhills' compliance with this DPA and/or Privacy and Data Protection Requirements, Sandhills agrees to allow for Customer to conduct an audit under Clause 12(a).

e) Request for audits should be directed to audits@sandhills.com.

f) Customer shall cover the cost of an audit conducted by itself or its third-party representatives.

g) The notice requirements in Clause 12(a) will not apply if the Customer reasonably believes that a Security Breach occurred or is occurring, or Sandhills is in breach of any of its obligations under this DPA or any Privacy and Data Protection Requirements.

13) Liability

a) Each Party's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the Limitation of Liability clause of the Terms.

14) Notices

a) Clause 14(b), does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

b) Any notices or other communications, unless they have specific methods of notice listed for them in this DPA, in regards to this DPA shall be delivered in writing to:

For Sandhills:

Email: Privacyresponse@sandhills.com

Mail: Sandhills Global, Inc.
Attn: Legal Department
120 West Harvest Drive
Lincoln, NE 68521

For Customer:

To the email address or mailing address for the primary billing contact listed in Sandhills' systems for Customer.

Exhibit 1 – Description of Processing

Nature and Purpose of Processing: Sandhills will Process Personal Data to provide Customer with the Hosted Website Services under the Terms. Sandhills will Process the Personal Data as a Processor, and engage sub-processors, as necessary to provide the Hosted Website Services pursuant to the Terms and this DPA. The purpose of the Processing is to service Customer and provide Hosted Website Services, supporting, and operating the provision of the Hosted Website Services.

Categories of Data Subjects: Sandhills may Process Personal Data under the Terms, which may include, but is not limited to the following categories of Data Subjects:

- Websites visitors
- Customer and their authorized employees or agents.

Categories of Data: Depending on the Customer's configuration, Sandhills may Process Personal Data under the Terms, which may include, but is not limited to the following categories of Personal Data:

- Contact Information (name, phone number, email, address, etc.)
- Internet or Similar Network Activity (IP Address, browser information, etc.)
- Device Information (Operating systems, device type, device capability information, geolocation, etc.)
- Messaging Information (Contents of messages to Customer from website visitors)

Duration of Processing: The Processing will occur on a continuous basis so long as the Terms are in effect, and for a period after in order for Sandhills to meet its obligations under this DPA.

Processing Operations: Sandhills will Process the Personal Data, which may include, collecting, storing, transferring, deleting, organizing, structing, altering, disclosing, and disseminating in order to provide the Hosted Website Services under the Terms. This includes the engagement of sub-processors as needed.

Exhibit 2 – EU SCCs

Standard Contractual Clauses – Controller to Processor (Module 2)

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.

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

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 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 [4] (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 to that list through the addition or replacement of sub-processors at least 30 calendar 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. (8) 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 subject.

(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 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 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.

(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 (12);

(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

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

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

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 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.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The Customer agreeing to the Terms.

Address: The address on file in Sandhills' customer management system for the Customer.

Contact person's name, position and contact details: The billing contact information on file in Sandhill's customer management system for the Customer.

Activities relevant to the data transferred under these Clauses: To receive the Hosted Website Services from Sandhills under the Terms.

Signature and date: The date on which the Customer agreed to the Terms.

Role: Controller

Data importer(s):

Name: The Sandhills Global entity which you are being billed by under the Terms.

Address: The address for the Sandhills Global entity which you are being billed by under the Terms.

Contact person's name, position and contact details: Scott McKinney, CIO, scott-mckinney@sandhills.com

Activities relevant to the data transferred under these Clauses: To provide the Hosted Website Services to the Customer under the Terms.

Signature and date: The date on which the Customer agreed to the Terms.

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Sandhills may Process Personal Data under the Terms, which may include, but is not limited to the following categories of Data Subjects:

- Websites visitors
- Customer and their authorized employees or agents.

Categories of personal data transferred

Depending on the Customer's configuration, Sandhills may Process Personal Data under the Terms, which may include, but is not limited to the following categories of Personal Data:

- Contact Information (name, phone number, email, address, etc.)
- Internet or Similar Network Activity (IP Address, browser information, etc.)
- Device Information (Operating systems, device type, device capability information, geolocation, etc.)
- Messaging Information (Contents of messages to Customer from website visitors)

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.

The collection of sensitive data is not envisioned under the Terms.

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

Personal data will be transferred on a continuous basis to provide the Hosted Website Services under the Terms.

Nature of the processing

Sandhills will Process the Personal Data, which may include, collecting, storing, transferring, deleting, organizing, structing, altering, disclosing, and disseminating in order to provide the Hosted Website Services under the Terms. This includes the engagement of sub-processors as needed.

Purpose(s) of the data transfer and further processing

Sandhills will Process Personal Data to provide Customer with the Hosted Website Services under the Terms. Sandhills will Process the Personal Data as a Processor, and engage sub-processors, as necessary to provide the Hosted Website Services pursuant to the Terms and this DPA. The purpose of the Processing is to provide Hosted Website Services to Customer, supporting, and operating the provision of the Hosted Website Services.

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

The Processing will occur on a continuous basis so long as the Terms are in effect, and for a period after in order for Sandhills to meet its obligations under this DPA or as otherwise lawfully directed by the Customer.

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

Sub-processors are used solely to deliver the products and services under the Terms.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Data Protection Commission (Ireland)

ANNEX II

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

See Exhibit 4 for the list of security measures.

ANNEX III

LIST OF SUB-PROCESSORS

See Exhibit 5 for the list of subprocessors.

Exhibit 3 – UK Addendum

Information Commissioner's Office

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

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	Date on which the Hosted Website Terms and Conditions were agreed to by Customer.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: See Annex I (A) of the EU SCCs. Trading name (if different): Main address (if a company registered address): See Annex I(A) of the EU SCCs.	Full legal name: See Annex I (A) of the EU SCCs. Trading name (if different): See brands page. Main address (if a company registered address): See Annex I(A) of the EU SCCs.

	Official registration number (if any) (company number or similar identifier):	Official registration number (if any) (company number or similar identifier): If Sandhills East LTD is the applicable Sandhills entity then Z313700X.
Key Contact	Full Name (optional): See Annex I(A) of the EU SCCs. Job Title: See Annex I(A) of the EU SCCs. Contact details including email: See Annex I(A) of the EU SCCs.	Full Name (optional): See Annex I(A) of the EU SCCs. Job Title: See Annex I(A) of the EU SCCs. Contact details including email: See Annex I(A) of the EU SCCs.
Signature (if required for the purposes of Section 2)	Signed as of the date the Customer agrees to the Hosted Website Terms and Conditions and the EU SCCs.	Scott Mckinney

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: The date the Customer agrees to the Hosted Website Terms and Conditions and the EU SCCs. Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See list of parties in Exhibit 2, Annex I(A).
Annex 1B: Description of Transfer: See description in Exhibit 2, Annex I(B).
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See description of measures taken in Exhibit 2, Annex II.
Annex III: List of Sub processors (Modules 2 and 3 only): See list of subprocessors in Exhibit 2, Annex III.

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.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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 of those Mandatory Clauses.

Exhibit 4 - Security Measures

This Exhibit 4 describes the technical and organizational measures maintained by Sandhills to protect Personal Data Processed in connection with the Hosted Website Services and related hosted service functionality. Measures are applied based on the nature, scope, context, and purpose of processing; data sensitivity; system capability; technical feasibility; and associated security and privacy risk.

The measures apply to Sandhills' managed Hosted Websites and supporting production systems, databases, operational records, support activity, logs, metadata, security telemetry, and administrative systems used to provide, secure, monitor, support, or administer the hosted services. Customer-owned systems, customer-controlled integrations, and third-party applications not managed by Sandhills remain outside Sandhills' operational control.

1. Security Governance and Accountability

Purpose: To maintain an information security and privacy governance program that supports appropriate protection of Personal Data processed in connection with the Hosted Website Services.

Measures include:

- Written information security and privacy policies, standards, or procedures
- Defined security, privacy, IT, development, infrastructure, and operational responsibilities
- Management oversight of significant security measures, risks, and technology changes
- Personnel confidentiality expectations and security awareness requirements
- Escalation paths for suspected security incidents, weaknesses, or policy exceptions
- Risk-based evaluation of safeguards based on system capability, data sensitivity, and operational context

2. User Identification and Authorization

Purpose: To limit access to systems and Personal Data to authorized users based on business need and job responsibility.

Measures include:

- Unique user IDs for interactive users where technically supported, with role- or responsibility-based access restrictions
- Authorization processes for access requests and permission changes, with administrative access limited to authorized personnel
- Separation of administrative access from standard user access where supported

- Multi-factor authentication for remote access, administrative access, Microsoft services, and supported cloud platforms where required by policy
- Periodic review of privileged, general user, shared, and service account access or records
- Access removal or modification upon termination, transfer, or change in business need
- Logging or monitoring of access activity where feasible

3. Encryption, Pseudonymization, and Data Protection

Purpose: To protect Personal Data using encryption and related safeguards appropriate to data sensitivity, system design, technical capability, and risk.

Measures include:

- TLS/HTTPS for applicable public-facing hosted services where supported
- Encryption at the storage, database, application, backup, or platform layer where supported and appropriate
- Protection of credentials, secrets, keys, and authentication materials based on sensitivity and system capability
- Masking, aggregation, deidentification, or minimization where appropriate and feasible
- Logical separation of environments, systems, datasets, or access paths
- Data classification and handling expectations based on sensitivity

4. Network, Platform, and Application Security

Purpose: To protect hosted service infrastructure and related administrative environments against unauthorized access, misuse, and service disruption.

Measures include:

- Network segmentation between corporate, internal server, DMZ, hosted service, and related environments
- Firewall enforcement and restricted network access using default-deny or equivalent traffic controls
- IDS/IPS, URL filtering, or equivalent perimeter protections
- VPN controls for administrative remote access
- Load balancing and traffic management for applicable hosted services
- Endpoint and email security controls for applicable systems and administrative environments
- Edge security services, such as Cloudflare, supporting DNS, CDN, WAF, bot mitigation, DDoS protection, traffic filtering, and TLS for applicable public-facing services

5. Data Storage, Minimization, Quality, Retention, and Disposal

Purpose: To manage data throughout its lifecycle in a manner consistent with service requirements, customer instructions, legal requirements, and operational feasibility.

Measures include:

- Storage of hosted service data in approved production and supporting systems with appropriate access restrictions
- Processing limited to hosted service delivery, support, security, administration, troubleshooting, improvement, legal, audit, backup, and continuity purposes
- Customer responsibility for the accuracy, lawfulness, appropriateness, and minimization of customer-provided content and Personal Data
- Normalization, validation, updating, correction, or disposal of data as needed to operate, support, secure, or improve the hosted services
- Retention of Personal Data for as long as needed for applicable agreement, privacy, operational, legal, security, backup, recovery, audit, or continuing business purposes
- Approved deletion, return, deidentification, or disposal requests handled subject to identity verification, customer instructions, legal exceptions, operational feasibility, backup retention, security requirements, and applicable law

6. Logging, Monitoring, and Incident Response

Purpose: To detect, investigate, respond to, document, and support escalation of security-relevant events affecting hosted services or related systems.

Measures include:

- Collection of security-relevant logs from applicable systems and tools
- Monitoring of identity, endpoint, network, infrastructure, application, VPN, firewall, database, cloud, and security tooling events
- Review of security alerts and events by responsible personnel or supporting security providers
- Triage and escalation of potential security events based on severity, business impact, legal considerations, and operational context
- Investigation, containment, remediation, and documentation of security incidents as appropriate
- Incident records that may include task orders, security tool output, communications, investigation notes, remediation actions, and post-incident review materials

- Coordination with Legal, leadership, or appropriate stakeholders for security or privacy incidents where applicable

7. System Configuration, Change Management, and Secure Development

Purpose: To maintain controlled configuration, change, and development processes for systems and applications supporting the services.

Measures include:

- Inventory or tagging of applicable assets, systems, applications, infrastructure, and platform components, including ownership and environment classification where maintained
- Configuration and patching records maintained through approved tools or processes
- Authorization and tracking of production changes prior to deployment through task orders, change records, deployment records, peer review records, maintenance records, configuration records, or equivalent operational records
- Controlled implementation of production changes, with testing before deployment and separation of production and non-production environments where feasible
- Emergency change documentation as soon as operationally feasible when immediate action is required to restore availability, address active security threats, or mitigate operational incidents

8. Testing, Vulnerability Management, and Assurance

Purpose: To regularly assess and evaluate the effectiveness of technical and organizational measures used to protect the services and Personal Data.

Measures include:

- Internal vulnerability scanning and agent-based visibility for applicable systems
- External attack surface monitoring, vendor advisory review, and threat intelligence
- Penetration testing or targeted security assessments based on system risk
- Periodic security control evaluations and risk assessments
- Management oversight and documented treatment of findings based on severity, exploitability, exposure, system criticality, data sensitivity, compensating controls, operational feasibility, and available remediation options, using remediation, mitigation, deferral, acceptance, muting, or other documented operational or management processes

9. Backup, Recovery, Availability, and Resilience

Purpose: To support restoration of critical systems and data following a physical, operational, technical, or security incident.

Measures include:

- Backup and recovery processes for applicable production systems and supporting services
- Production backup platforms and recovery tooling
- Ransomware recovery support
- Microsoft 365 backup services
- Off-site media storage
- Vendor-supported backup or recovery services
- Business continuity and disaster recovery planning for applicable critical systems
- Recovery prioritization based on system criticality, data integrity, security validation, customer impact, business impact, and operational feasibility
- Specific uptime, restoration, recovery time, or recovery point commitments only where separately stated in the applicable agreement

10. Physical and Environmental Security

Purpose: To protect company-controlled facilities, data center spaces, office areas, and physical media supporting hosted services.

Measures include:

- Authorized and restricted physical access to sensitive areas and company-controlled data center spaces
- Visitor management expectations
- Physical and environmental safeguards for systems and media supporting hosted services
- Physical media handling and disposal controls
- Use of geographically distinct company-operated data center operations to support resilience
- Risk-based review of third-party facility or service controls through vendor management, contractual terms, service agreements, assurance documentation, complementary subservice organization controls, or equivalent methods

11. Subprocessors and Customer Assistance

Purpose: To manage vendors and subprocessors that support the services or Process Personal Data, and to provide reasonable assistance to customers with applicable privacy, security, and audit-related obligations.

Measures include:

- Risk-based vendor and subprocessor evaluation, including review of available SOC, ISO, PCI, trust center, security, privacy, or equivalent assurance materials where appropriate
- Contractual confidentiality, security, privacy, or data protection obligations appropriate to the service
- Subprocessor obligations materially consistent with applicable security and data protection obligations
- Assistance with applicable privacy rights, security, incident, and audit-related requests, including but not limited to, access, portability, correction, deletion, or erasure, subject to customer instructions, identity verification, legal exceptions, operational feasibility, backup retention, security requirements, confidentiality obligations, and applicable law
- Maintenance of records or information reasonably necessary to support security, privacy, audit, and vendor governance activities

12. Control Applicability

The measures in this Exhibit describe Sandhills' general technical and organizational measures for the services and may not apply uniformly to every system, dataset, environment, customer, hosted site, or processing activity. Applicability is determined based on system design, technical capability, business purpose, data sensitivity, risk, service configuration, customer instructions, and operational feasibility.

Sandhills may update or replace measures from time to time, provided that such updates do not materially reduce the overall level of security provided for the hosted services during the applicable agreement term.

Exhibit 5 - Subprocessors

Subprocessor	Activities	Location of Processing
Cloudflare	Provides network proxy, DNS Hosting, and CDN services.	Global
Google	Provides infrastructure for analytics, Tag Management, and ReCAPTCHA.	Global
Sandhills Global, Inc.	Provides various support services, including but not limited to, data processing, design and development services.	US
Azure O365	Provide E-mail services related to Hosted Websites.	US
Shopify	Provides optional eCommerce Features for Hosted Websites.	US, Canada and EU
Osano	Provides CMP Solution for Hosted Websites.	Global

Subprocessor Web Page

Last Updated: September 15, 2026

V9-10-2026