INTERNATIONAL DATA PROCESSING AGREEMENT

Effective on October 29, 2025 (the "Effective Date")

This International Data Processing and Transfer Agreement ("Data Processing Agreement") is entered into between you and the entity you represent ("Data Controller", "Company", "you" or "your"), and the Service Provider, 2ndSite Inc., doing business as FreshBooks, a Canadian company located at 225 King St. W, #1200, Toronto, Ontario, M5V 3M2 ("Data Processor") in connection with Service Provider's provision of services to Company, pursuant to any applicable Terms of Service (defined below) between the parties and consisting of software Services (defined below).

The Data Controller and the Data Processor hereby agree as follows:

1. Subject matter of this Data Processing Agreement

1.1 This Data Processing Agreement applies to the processing of (i) personal data that is subject to Regulation (EU) 2017/679 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, and repealing Directive 95/46/EC (General Data protection Regulation ("EU Data Protection Law"), (ii) personal information that is subject to the California Consumer Privacy Act of 2018 ("CCPA"), and (iii) personal information that is subject to the Canadian privacy laws, including the Personal Information Protection and Electronic Documents Act (Canada), the Personal Information Protection Act (Alberta), the Personal Information Protection Act (British Columbia) and, the Act respecting the protection of personal information in the private sector (Québec) (collectively the "Canadian Privacy Laws"). The EU Data Protection Law, CCPA and Canadian Privacy Laws are collectively referred to as the "Applicable Data Protection Law" within the scope of the agreement for the use of the software Data Processor provides – including but not limited to invoicing, time tracking, expense tracking, invoice payments, accounting reporting, and the API ("Services") ("Terms of Service").

1.2 Capitalized terms used but not defined in this Data Processing Agreement shall have the meanings set forth in Applicable Data Protection Law. "Personal Data" means any information relating to an identified or identifiable natural person, including information that constitutes "personal information" under Applicable Data Protection Law.

1.3 Insofar as the Data Processor will be processing Personal Data subject to Applicable Data Protection Law on behalf of the Data Controller in the course of the performance of the Services under the Terms of Service with the Data Controller, the terms of this Data Processing Agreement shall apply. For EU Data Protection Law, an overview of the categories of Personal Data, the types of Data Subjects, and purposes for which the Personal Data are being processed is provided in Annex 2.

2. The Data Controller and the Data Processor

2.1 The Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor. The Data Processor will process the Personal Data only as set forth in Data Controller's written instructions or as otherwise permitted under Applicable Data Protection Law.

2.2 The Data Processor will only process the Personal Data on documented instructions of the Data Controller in such manner as - and to the extent that - this is appropriate for the provision of the Services and in the context of the Company's direct business relationship with the data subject, except as required to comply with a legal obligation to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of that legal obligation before processing, unless that law explicitly prohibits the furnishing of such information to the Data Controller. Except as required to comply with Applicable Data Protection Law, the Data Processor shall never process the Personal Data in a manner inconsistent with the Data Controller's documented instructions. Where the Data Processor is subject to EU Data Protection Law, it shall immediately inform the Data Controller if, in its opinion, an instruction infringes EU Data Protection Law or other EU or EU Member State data protection provisions.

2.3 The Parties have entered into the Terms of Service in order to benefit from the expertise of the Data Processor in securing and processing the Personal Data for the purposes set out in Annex 2. The Data Processor shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this Data Processing Agreement.

2.4 Company agrees to comply with all laws applicable to it as Controller. Data Controller warrants that it has all necessary rights to provide the Personal Data to Data Processor for the Processing to be performed in relation to the Services. To the extent required by Applicable Data Protection Law or other applicable privacy and data protection laws, Data Controller is responsible for ensuring that any necessary data subject notices of this Processing are given and consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by the data subject, Data Controller is responsible for communicating the fact of such revocation to the Data Processor, and Data Processor remains responsible for implementing any Data Controller instruction with respect to the further processing of that Personal Data.

3. Confidentiality

3.1 Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as strictly confidential and it shall inform all its employees, agents and/or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, without prejudice to any other security standards agreed upon by the Parties, the Data Controller and Data Processor shall implement reasonable technical and organisational measures, in compliance with Applicable Data Protection Law, designed to protect the Personal Data, taking into account its sensitivity and the associated risk. These measures shall include as appropriate:

(a) measures to ensure that the Personal Data can be accessed only by authorized personnel for the purposes set forth in Annex 2 of this Data Processing Agreement;

(b) in assessing the appropriate level of security, account shall be taken of the sensitivity of Personal Data and, in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Personal Data;

(c) the pseudonymisation and encryption of Personal Data;

(d) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(e) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(f) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of Personal Data;

(g) the measures agreed upon by the Parties in Annex 3, if any.

4.2 The Data Processor shall at all times have in place an appropriate written security policy with respect to the processing of Personal Data, outlining in any case the measures set forth in Article 4.1.

4.3 Upon Data Controller's written request at reasonable intervals, the Data Processor shall provide a copy of its then most recent third party audits or certifications, as applicable, or any summaries thereof, related to the processing of Personal Data of Company, that the Data Processor generally makes available to its customers at the time of such request. The Data Processor shall make available to Company, upon reasonable written request, such information necessary to demonstrate compliance with this Data Processing Agreement, and shall allow for written audit requests by Data Controller or an independent auditor in relation to the processing of Personal Data to verify that the Data Processor employs reasonable procedures in compliance with this Data Processing Agreement, provided that Company shall not exercise this right more than once per year. Such information and audit rights are provided under this section 4.3 to the extent the Data Processing Agreement does not provide such audit rights that meet the requirements of EU Data Protection Law. Any information provided by the Data Processor and/or audits performed pursuant to this section are subject to the confidentiality obligations set forth in this Data Processing Agreement.

5. Improvements to Security

5.1 The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Article 4 on an on-going basis and will tighten, supplement and improve these measures in order to maintain compliance with the requirements set out in Article 4. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in Applicable Data Protection Law or by data protection authorities of competent jurisdiction.

5.2 Where an amendment to the Terms of Service is necessary in order to execute a Data Controller instruction to the Data Processor to improve security measures as may be required by changes in Applicable Data Protection Law from time to time, the Parties shall negotiate an amendment to the Service Agreement in good faith.

6. Data Transfers Out of the European Economic Area

6.1 The Data Processor shall immediately notify the Data Controller of any (planned) permanent or temporary transfers of Personal Data from a country inside of the European Economic Area to a country outside of the European Economic Area without an adequate level of protection and shall only perform such a (planned) transfer after obtaining authorisation from the Data Controller, which may be refused at its own discretion. Annex 4 provides a list of data transfer types for which the Data Controller grants its consent upon the conclusion of this Data Processing Agreement and the relevant appropriate safeguards, such as standard contractual clauses which are enclosed in Annex 5.

6.2 To the extent that the Data Controller or the Data Processor are relying on a specific statutory mechanism to normalize the international data transfers in section 6.1 and such mechanism is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Data Controller and the Data Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support such transfer.

7. Information Obligations and Incident Management

7.1 When the Data Processor becomes aware of an incident that impacts the Processing of the Personal Data that is the subject of the Services Agreement, it shall promptly notify the Data Controller about the incident, shall at all times reasonably cooperate with the Data Controller in the investigation and management of such incident, and shall follow the Data Controller's reasonable instructions with regard to such incidents, in order to enable the Data Controller to perform a thorough investigation into the incident, to formulate a response, and to take suitable further steps in respect of the incident.

7.2 The term "incident" used in Article 7.1 shall be understood to mean in any case:

(a) a complaint or a request with respect to the exercise of a data subject's rights under Applicable Data Protection Law;

(b) an investigation into or seizure of the Personal Data by government officials, or a specific indication that such an investigation or seizure is imminent;

(c) any unauthorized access or disclosure, unauthorized, unlawful or accidental loss, misuse, destruction, acquisition of, or damage to Personal Data, or any other unauthorized Processing of Personal Data;

(d) any breach of the security and/or confidentiality as set out in Articles 3 and 4 of this Data Processing Agreement leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or being about to take place;

(e) where, in the opinion of the Data Processor, implementing an instruction received from the Data Controller would violate applicable laws to which the Data Controller or the Data Processor are subject.

7.3 The Data Processor shall at all times have in place written procedures which enable it to promptly respond to the Data Controller about an incident. Where the incident is reasonably likely to require a data breach notification by the Data Controller under Applicable Data Protection Law, the Data Processor shall implement its written procedures in such a way that it is in a position to notify the Data Controller no later than 72 business hours of having become aware of such an incident.

7.4 Any notifications made to the Data Controller pursuant to this Article 7 shall be addressed to the employee of the Data Controller whose contact details are provided in Annex 1 of this Data Processing Agreement, and shall contain:

(a) a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained;

(c) a description of the likely consequences of the incident; and

(d) a description of the measures taken or proposed to be taken by the Data Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

8. Contracting with Sub-Processors

8.1 The Data Controller authorises the Data Processor to engage the sub- processors in the country locations for the Service-related activities specified as described in Annex 2, if any. Data Processor shall inform the Data Controller of any addition or replacement of such sub- processors giving the Data Controller an opportunity to object to such changes.

8.2 Notwithstanding any authorisation by the Data Controller within the meaning of the preceding paragraph,the DataProcessor shall remain fully liable vis-à-vis the Data Controller for the performance of any such subprocessor that fails to fulfil its data protection obligations.

8.3 The consent of the Data Controller pursuantto section 8.1 shall not alter the fact that consent is required under section 6 for the engagement of sub-processors in a country outside the European Economic Area without a suitable level of protection for applicable data transfers.

8.4 The Data Processor shall ensure that the sub-processor is bound by the same data protection obligations of the Data Processor under this Data Processing Agreement, shall supervise compliance thereof, and must in particular impose on its sub-processors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Applicable Data Protection Law.

8.5 The Data Controller may request that the Data Processor audit its sub-processor or provide confirmation that such an audit has occurred (or, where available, obtain or assist Data Controller in obtaining a third party audit report concerning the Third Party Subprocessor's operations) to ensure compliance with its obligations imposed by the Data Processor in conformity with this Data Processing Agreement.

9. Returning or Destruction of Personal Data

9.1 Unless otherwise permitted, upon termination of this Data Processing Agreement, upon the Data Controller's written request, or upon fulfillment of all purposes agreed in the context of the Services whereby no further processing is required, the Data Processor shall, at the discretion of the Data Controller, either delete, destroy or return all Personal Data to the Data Controller and destroy or return any existing copies.

9.2 The Data Processor shall notify all sub-processors supporting its own processing of the Personal Data of the termination of the Data Processing Agreement and shall ensure that all such sub-processors shall either destroy the Personal Data or return the Personal Data to the Data Controller, at the discretion of the Data Controller.

10. Assistance to Data Controller

10.1 The Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights under Applicable Data Protection Law.

10.2 The DataProcessor shall assistthe Data Controller in ensuring compliance with the obligations pursuant to Section 4 (Security) and prior consultations with supervisory authorities required under Article 36 of the EU Data Protection Law, when applicable, taking into account the nature of processing and the information available to the Data Processor.

11. Liability and Indemnity

11.1 The Data Processor indemnifies the Data Controller and holds the Data Controller harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Controller and arising directly or indirectly out of or in connection with a breach of this Data Processing Agreement and/or the Applicable Data Protection Law by the Data Processor. The Data Controller indemnifies the Data Processor and holds the Data Process harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Processor and arising directly or indirectly out of or in connection with a breach of this Data Processing Agreement and/or the Applicable Data Protection Law by the Data Controller.

12. Duration and Termination

12.1 This Data Processing Agreement shall come into effect on the Effective Date.

12.2 Termination or expiration of this Data Processing Agreement shall not discharge the Data Processor from its confidentiality obligations pursuant to Article 3.

12.3 The Data Processor shall process Personal Data until the date of termination of this Data Processing Agreement, unless instructed otherwise by the Data Controller, or untilsuch data isreturned or destroyed on instruction of the Data Controller.

12.4 The Data Processor may retain Personal Data beyond the date of termination of this Data Processing Agreement in accordance with Applicable Data Protection Laws, legal, and compliance requirements. In addition, the Data Processor will make reasonable efforts to return or destroy the data once it is deemed unnecessary for enforcement of laws, legal, and compliance requirements.

13. Miscellaneous

13.1 In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the Terms of Service, the provisions of this Data Processing Agreement shall prevail.

13.2 This Data Processing Agreement is governed by the laws of the MemberState in which the data exporter is established. Any disputes arising from or in connection with this Data Processing Agreement shall be brought exclusively before the

competent court.

13.3 This Data Processing Agreement may be executed in several counterparts (including delivery via facsimile or electronic mail), each of which will be deemed to be an original but all of which together will constitute one and the same instrument. Each party warrants that the execution and performance of its obligations under this Agreement does not conflict with or violate any other instrument, contract,
agreement, or other commitment or arrangement to which it is a party or by which it is bound, and that it knows of no other fact or circumstance that prevents it from entering into this Agreement.

Annex 1
ContactInformation

Contact information of the data protection officer of the Data Processor.

Davina Furnish
Chief Legal Officer
FreshBooks
dpo@freshbooks.com

Annex 2
Purposes of Processing

Personal Data that will be processed in the scope of the Terms of Service and the purposes for which these data will be processed:

CUSTOMER DATA

Data subjects

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

- Existing and prospective customers website visitors and end users of Company's technological offerings (e.g., web applications, mobile applications, API, payments).

Categories of data

The personal data transferred concern the following categories of data:

- General Identification Information: Name, physical address, email address, telephone number, avatar image, demographic characteristics (including birthdate, age and gender); profession (including salary);
- Operational Data: Staff, client, and accounting information (including invoices, invoice comments, expenses, expense receipts, and estimates); agreements, imported

bank expenses, payment and transaction information, including bank and credit card details, and any other information relevant to payment, billing and transactional purposes;

- Preferences: Information relating to a customer's preferences and profile, including product preferences, language preferences, interest in receiving communications, products and services; involvement in company programs/initiatives and any other data relevant to Company's relationship with the data subject; and

- Information Technology Data: Including online account information (e.g., username and password); information about website (including social media) and application browsing, activity, preferences, history, and interactions with Company products and services, device information (e.g., device identifiers,
  configuration, operating system, MAC addresses, IP addresses, serial numbers, RSSI information); and geolocation and itinerary tracking information, collected from fixed and mobile devices (e.g. mobile phones, wearables), online forms, cookies, pixel tags and other online tracking technologies.

Sensitive data

The personal data transferred concern the following categories of sensitive data:

- Sensitive data as required and permitted by applicable law, including data that may be relevant for a particular transaction with the customer.

Processing operations

The transfer is made for the following purposes:

- Communications: Facilitating communication with customers and their personnel; providing and improving customer services; marketing products and services to customers; contacting customers as necessary regarding their transactions, changes to Company's terms, conditions and policies or for other business administration purposes;

- Business Operations: Providing services to customers and processing transactions; operating and managing IT and communications systems (including customer account profiles); improving products, services and technological

offerings; designing and improving workflow; conducting business intelligence, including analysing market trends and statistics, running or facilitating surveys and product reviews; running marketing campaigns, tailoring customer experiences (online compiling audit trails and other reporting tools; conducting strategic planning; project management; offering customer support; and

- Compliance: (i) Complying with legal and other requirements, such as income tax and national insurance deductions; recordkeeping and reporting obligations; conducting audits; facilitating compliance with government inspections and responding to other requests from government or other public authorities; responding to legal process such as subpoenas; pursuing legal rights and remedies; defending litigation and managing any internal complaints or claims, conducting internal investigations, including as to reports of allegations of wrongdoing, policy violations, fraud, or financial reporting concerns (including whistleblowing schemes) and global business continuity plan; and complying with internal policies and procedures; (ii) protecting, enforcing or defending the legal rights, privacy, safety, or property of Company, Company affiliates or their employees, agents and contractors (including enforcement of relevant agreements and terms of use); (iii) protecting the safety, privacy, and security of users of Company products or services or members of the public; and addressing malfunctions or issues with Company's technological offerings or infrastructure; or (iv) protecting against fraud or for risk management purpose.

Annex 3
Security measures

The Data Processor applies the following security and reliability safeguards:
https://www.freshbooks.com/policies/security-safeguards.
These safeguards will be updated from time to time.

Annex 4
Data Transfer Types to Other Countries

Transfers to countries outside the European Economic Area (EEA) without a suitable level of protection for which the Data Controller has granted its authorisation

The following are the vendor categories used to provide services, that might require data.

Vendor Categories and the Relevant appropriate safeguards

taken for each vendor type

#	Vendor Type	Type of Data	Privacy Controls in Place
A	Sub processors established in EEA	Personal and sensitive Information	Decision. Offer higher or equivalent controls to GDPR for data privacy
B	Sub processors established in countries covered in Adequacy Decision	Personal and sensitive Information	
C	Sub Processors established in countries not covered in Adequacy	Personal and sensitive Information GDPR compliant	Data Processing Agreement (DPA) and Standard Contractual Clauses (SCC) are in place as per Annex 5.
D	Other Sub Processors	Processing non-personal information	Not Applicable

Note: Vendors from all the above categories are utilized to provide our services. Vendors of Category C are currently located in the US.

Note: The official SCC can be found here

Annex 5

Standard Contractual Clauses for the transfer of personal data to processors in third countries between Company (Data Controller) and 2ndSite Inc. doing business as FreshBooks (Data Processor)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as “Company” in the DPA
(the “data exporter”)

and

2ndSite Inc.
225 King St W, #1200, Toronto, Ontario, M5V 3M2
(the “data importer”)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data

exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) 'the data exporter' means the controller who transfers the personal data; (c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1) The data subject can enforce against the data exporter this Clause, Clause

4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2) The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3) The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub processor shall be limited to its own processing operations under the Clauses. 4) The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract; (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing

adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub processor providing at least the same level of
protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be

carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

by the data exporter, where applicable, in agreement with the supervisory authority; (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1) The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2) If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
3) If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses

as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1) The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2) The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1) The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2) The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3) The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Sub-processing

1) The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[2]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2) The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3) The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4) The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services 1) The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2) The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

[2] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Appendix 1 to the Standard Contractual Clauses

Data exporter

The data exporter is the entity identified as “Data Controller” or “Company” in the Data Processing Agreement (DPA).

Data importer

The data importer is the entity identified as “Data Processor” in the DPA.

Data subjects

Data subjects are defined in Section 1.3 of the DPA.

Categories of data

Categories of data are defined in Section 1.3 of the DPA.

Special categories of data (if appropriate)

Not collected hence not applicable

Processing operations

The personal data transferred will be subject to processing as defined in Section 1.3 of the DPA.

Appendix 2

to the Standard Contractual Clauses

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

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):

The Data Processor applies the following security and reliability safeguards:
https://www.freshbooks.com/policies/security-safeguards.
https://www.freshbooks.com/policies/privacy

These safeguards will be updated from time to time.