wasabi

# DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "**Data Processing Agreement**" or "**DPA**") supplements the separate agreement (the "**Services Agreement**") governing the provision of Services (as defined below). This DPA is an agreement between you or the entity you represent ("**Customer**") and Wasabi Technologies LLC ("**Wasabi**") and applies when one or more Data Protection Laws apply to Wasabi's Processing Personal Data as a result of Customer's access and use of Wasabi's cloud storage services (the "**Services**"). This Data Processing Agreement refers to Customer and Wasabi individually as a "**Party**" and collectively as the "**Parties**."

By using the Services or by clicking "accept" or "agree" to this DPA when this option is made available, you accept and agree to be bound and abide by this DPA. If you do not want to agree to this DPA, you may terminate your use of the Services in accordance with the Services Agreement.

**1.** **DEFINITIONS.** Capitalized terms used and not defined in this Data Processing Agreement have the respective meanings assigned to them in the Services Agreement.

"**Affiliate**" means any entity that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the Party. For purposes of this definition, the term "control" means the power (or, as applicable, the possession or exercise of the power) to direct, or cause the direction of, the management, governance, or policies of a given entity, directly or indirectly, through any applicable means (whether through the legal, beneficial, or equitable ownership, of more than fifty percent (50%) of the aggregate of all voting or equity interests or securities of such entity, through partnership, or through some other form of ownership interest, by contract, or other applicable legal document, or otherwise).

"**Applicable Law**" means any international, foreign, national, federal, state, or local statutes, ordinances, regulations, rules, executive orders, supervisory requirements, directives, circulars, opinions, judgments, interpretive letters, official releases, and other pronouncements having the effect of law and requirements or standards issued by a self-regulatory organization which apply from time to time to the person or activity in the circumstances in question. Applicable Law includes any of the foregoing as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

"**CCPA**" means the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 et seq.), as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

"**Colorado CPA**" means the Colorado Consumer Privacy Act of 2021 (Col. Rev. Stat. 6-1-13 et seq.), as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

"**Controller**" means either: (a) the meaning set forth in the relevant Data Protection Laws; or (b) absent such a definition, the Party that, alone or jointly with others, determines the means and purpose of the Processing of Personal Data. Without limiting the foregoing, the term "Controller" includes a "business" under the CCPA or CPRA.

"**CPRA**" means the California Consumer Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 et seq.), as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

"**Data Protection Laws**" means any Applicable Law relating to Personal Data or collection, use, storage, disclosure, transfer, or other Processing of Personal Data of or by any government, or any authority, department, or agency thereof, or self-regulatory organization, including, without limitation: (a) GDPR; (b) UK GDPR; (c) CCPA; (d) PIPEDA; (e) CPRA (when in effect); (f) Virginia CDPA (when in effect); and (g) Colorado CPA (when in effect).

"**Data Subject**" means either: (a) the meaning set forth in the relevant Data Protection Laws; or (b) absent such a definition, the individual who is the subject of Personal Data that Wasabi Processes for Customer. Without limiting the foregoing, the term "Data Subject" includes a "consumer" as defined under the CCPA or CPRA.

"**EU Standard Contractual Clauses**" or "**EU-SCCs**" means the applicable module(s) of the European Commission's standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as set out in the Annex to Commission Implementing Decision (EU) 2021/914, a completed copy of which comprises Exhibit 1, as amended, supplemented or otherwise modified from time to time.

"**GDPR**" means the EU General Data Protection Regulation (EU Regulation 2016/279) and the implementing acts of the foregoing by a Member State, Switzerland, each as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

"**Member State**" means a member state of the European Union and/or the European Economic Area, as may be amended from time to time.

"**Personal Data**" means any information Wasabi Processes for Customer (other than contact information for Customer or Customer's personnel) that: (a) the relevant Data Protection Laws otherwise define as "personal information" or "personal data."; or (b) in absence of such a definition in the relevant Data Protection Laws, such information that identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Wasabi's possession or control or that Wasabi is likely to have access to. Without limiting the foregoing, the term "Personal Data" includes any "personal data" as defined under the GDPR and any "personal information" as defined under the CCPA and the CPRA. Without limiting the foregoing, Personal Data includes the Data Subject's name, an identification number, geo-location data, an online user identification.

"**PIPEDA**" means the Canadian Personal Information Protection and Electronics Documents Act, as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

"**Process**" means either: (a) the meaning set forth in the relevant Data Protection Laws; or (b) absent such a definition, any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction. Processing also includes transferring Personal Data to third-parties. The terms "**Processing**" and "**Processed**" have a correlative meaning.

"**Processor**" means either: (a) the meaning set forth in the relevant Data Protection Laws; or (b) absent such a definition, the Party that Processes the Personal Data on behalf of the Controller. Without limiting the foregoing, the term "Processor" includes a "service provider" or a "contractor" under the CCPA or CPRA.

"**Security Incident**" means any act or omission that materially compromises or is reasonably likely to materially compromise either the security, confidentiality, or integrity of Personal Data or the physical, technical, administrative, or organizational safeguards put in place by Wasabi, that relate to the protection of the security, confidentiality, or integrity of Personal Data. Without limiting the foregoing, a material compromise includes any accidental, unlawful, or unauthorized use, modification, loss, compromise, destruction, or disclosure of, or access to, Personal Data. Notwithstanding the foregoing, the term "Security Incident" does not include any event that does not result in any unauthorized access to Personal Data or to Wasabi's equipment or facilities storing Personal Data, including, without limitation, pings and other broadcast attacks on firewalls or other network equipment, port scans, unsuccessful logon attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond communication headers) or similar incidents.

"**Standard Contractual Clauses**" means the EU Standard Contractual Clauses and/or the UK Standard Contractual Clauses, as applicable.

"**Subprocessor**" means a third-party engaged by Wasabi to assist with the provision of the Services which involves the Processing of Personal Data.

"**UK GDPR**" means the United Kingdom Data Protection Act of 2018 and the United Kingdom General Data Protection Act, as amended from time to time and any successor legislation thereto and any regulations promulgated thereunder.

"**UK Standard Contractual Clauses**" or "**UK-SCC**" means the European Commission's Standard Contractual Clauses for the transfer of Personal Information from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU, as may be amended, modified, or replaced by the United Kingdom, a completed copy of which comprises Exhibit 2, as amended, supplemented or otherwise modified from time to time.

"**Virginia CDPA**" means the Virginia Consumer Data Protection Act of 2021 (Virginia Code § 59.1-571 et seq.).

**2.** **RELATIONSHIP WITH SERVICES AGREEMENT.** If Customer is a party to the Agreement, this DPA is subject to the terms of the Services Agreement and is hereby incorporated into the Services Agreement. If Customer has executed an Order with Wasabi pursuant to the Agreement, but is not itself a party to the Agreement, then this DPA is an addendum to that Order and all applicable renewal Orders. All related exhibits, schedules, attachments, appendices, and any other documents incorporated herein by reference (collectively, the "**Addendum**") 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 such Addendum. Notwithstanding anything to the contrary in the Services Agreement, in case of a conflict, inconsistency, or ambiguity between the Standard Contractual Clauses, the Addendum, and the body of this DPA, the following order of precedence governs: (a) first, the Standard Contractual Clauses; (b) second, the body of this DPA (to the extent this DPA requires additional, more stringent, or more protective obligations than the Addendum or the Services Agreement); (c) third, the Addendum; and (d) fourth, the Services Agreement.

**3.** **RELATIONSHIP OF THE PARTIES.** Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Laws, including providing any required notices and obtaining any required consents (except to the extent explicitly set forth in the Services Agreement), and for the Processing instructions it gives to Wasabi. The Parties acknowledge and agree that with regard to the Processing of Personal Data (other than contact information of Customer or Customer's personnel, for which the Parties are independent controllers), Wasabi is the "Processor" and Customer is the "Controller" under this Data Processing Agreement.

## 4. CUSTOMER OBLIGATIONS.

**4.1.** **Compliance with Laws.** Customer shall, in its use of the Services, Process the Personal Data in accordance with the requirements of applicable Data Protection Laws.

**4.2.** **Licenses and Registrations.** Customer shall obtain all material licenses, authorizations, approvals, consents, or permits required of it as a Controller under applicable Data Protection Laws to Process the Personal Data as set forth in this DPA, the Services Agreement, or as required under Data Protection Laws and to perform its obligations under this DPA or the Services Agreement.

**4.3.** **Customer Instructions.** Customer's instructions to Wasabi for the Processing of Personal Data will comply with Data Protection Laws and Customer will have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

**4.4.** **Data Protection Officers and Representatives.** To the extent required by applicable Data Protection Laws, Customer shall appoint data protection representative and/or data protection officers in all applicable jurisdictions.

## 5. WASABI'S OBLIGATIONS.

**5.1.** **Scope of Processing.** The nature, scope, and purpose of the Processing of Personal Data is set forth in Schedule A.

**5.2.** **Compliance with Data Protection Laws.** Wasabi will comply in all material respects with applicable Data Protection Laws with respect to its Processing of Personal Data and provision of the Services.

**5.3.** **Licenses and Registrations.** Wasabi shall obtain all material licenses, authorizations, approvals, consents or permits required of it as a Processor under applicable Data Protection Laws to perform its obligations and Process the Personal Data under this DPA and the Services Agreement.

**5.4.** **Data Protection Officers and Representatives.** To the extent required by applicable Data Protection Laws, Wasabi shall appoint one or more data protection representatives and/or data protection officers in the applicable jurisdictions.

**5.5.** **Limited Processing; Confidentiality.** Wasabi agrees and covenants that it shall: (a) not create, collect, receive, access, use, or otherwise Process the Personal Data in violation of any Applicable Law (including Data Protection Laws); (b) Process the Personal Data solely and exclusively for the purposes for which the Personal Data, or access to it, is provided pursuant to the terms and conditions of the Services Agreement and this DPA; and (c) not collect, retain, use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Data outside of the direct business relationship with Customer or for Wasabi's own purposes or for the benefit of anyone other than Customer's, in each case, without Customer's prior written consent. Notwithstanding the foregoing, unless explicitly prohibited by Customer in writing (including under the Services Agreement or this DPA), Wasabi may use the Personal Data as follows to the extent permitted by applicable Data Protection Laws: (i) for its internal use to build or improve the quality of the Services provided by Wasabi, provided, however, that Wasabi does not use the Personal Data to build or modify a profile about a Data Subject or their household to use in providing services to a third-party, or cleaning or augmenting any Personal Data acquired from another source; (ii) to detect Security Incidents, or to protect against fraudulent or illegal activity; (iii) as otherwise explicitly permitted under Data Protection Law; and (iv) to respond to any Legal Order.

**5.6.** **Instructions from Customer.** Wasabi shall only Process the Personal Data to the extent, and in such a manner, as is necessary to perform the Services in accordance with Customer's documented instructions. Customer may provide Wasabi with general or specific data protection-related instructions. Wasabi shall not Process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Laws. To the extent permitted by Applicable Law, Wasabi shall promptly notify Customer if, in its reasonable opinion, Customer's instruction would not comply with the Data Protection Laws. Without limiting the foregoing, Customer hereby instructs Wasabi to Process the Personal Data for the following purposes: (a) as necessary for the provision of the Services and in accordance with this DPA and the Services Agreement; (b) as initiated by Customer's end users in their use of the Services; (c) to comply with other reasonable instructions provided by Customer to Wasabi (e.g., via email or via support requests) where such instructions are consistent with the terms of the Services Agreement and this DPA; and (d) to respond to a Legal Order.

5.7. **Excess Processing Requirements.** In the event Wasabi is required under any applicable Data Protection Law to Process the Personal Data in excess of Customer's documented instructions, Wasabi shall immediately notify Customer of such a requirement, unless such applicable Data Protection Law prohibits such notification, in which case Wasabi shall notify Customer of this required Processing as soon as the applicable Data Protection Law permits it to do so.

5.8. **Inability to Comply.** Wasabi shall promptly inform Customer in the event Wasabi cannot reasonably provide compliance with this Data Processing Agreement for whatever reason. In such an event, Customer may immediately suspend any Processing of Personal Data and/or terminate the Services pursuant to the Services Agreement.

5.9. **Assistance in Compliance with Obligations under Data Protection Laws.** Taking into account the nature of Wasabi's Processing and the information available to Wasabi, Wasabi shall reasonably assist Customer in meeting Customer's compliance obligations under the Data Protection Laws (including, without limitation, Customer's security requirements, notifications or other communications related to any Security Incidents, responding to Data Subject Requests, and any data privacy impact assessments and/or prior consultations with supervisory authorities or other competent data privacy authorities provided for under applicable Data Protection Laws) through appropriate technical and organizational measures. Wasabi reserves the right to invoice, and Customer shall pay, for any additional costs arising from Wasabi's provision of such assistance.

5.10. **Cooperation with Regulators.** At Customer's sole cost and expense, Wasabi and its representatives shall cooperate, upon request from Customer, with any and all requests from data protection authorities and regulators having jurisdiction over Customer, including those with jurisdiction to monitor and ensure compliance with applicable Data Protection Laws.

5.11. **Requests from Customer.** Wasabi shall promptly comply with any Customer request or instruction requiring Wasabi to amend, transfer, delete, or perform any other lawful Processing of Personal Data, and to stop, mitigate, or remedy any unauthorized Processing.

5.12. **Data Analytics; Anonymized Personal Data.** Any data collected pursuant to data analytics or monitoring carried out by Wasabi in connection with the provision of the Services or otherwise connected with Customer's use of the Services may include Personal Data. Wasabi may aggregate, de-identify, or anonymize Personal Data and use such aggregated, de-identified, or anonymized data, which shall no longer be considered Personal Data, for its own reasonable purposes. Customer hereby authorizes Wasabi to Process the Personal Data for the purposes described in this Section 5.12.

## 6. COMPLAINTS; DATA SUBJECT REQUESTS; AND THIRD PARTY RIGHTS.

6.1. **Complaints and Other Communication.** Wasabi shall notify Customer in the event it receives any request, complaint, or communication relating to Customer's obligations under Data Protection Laws (including from data protection authorities and/or supervisory authorities). To the extent permitted by applicable Data Protection Laws, Wasabi shall obtain specific written consent and instructions from Customer prior to responding to such request, complaint, or communication.

6.2. **Data Subject Requests Received by Wasabi.** Wasabi shall, to the extent permitted under Applicable Law, promptly notify Customer if Wasabi receives a request from a Data Subject or their representative to exercise any rights provided to Data Subject with respect to their Personal Data under applicable Data Protection Laws, including, but not limited to, any rights of access, rectification, erasure, data portability, or restriction of Processing, right to object to Processing, right to not have their Personal Data shared or sold, or not to be subject to automated decision making ("**Data Subject Request**").

**6.3.** **Assistance with Data Subject Requests.** Taking into account the nature of the Processing, Wasabi shall provide all reasonable assistance to Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Laws. The parties agree and acknowledge that Wasabi may, but is not required to, fulfill its obligations described in the foregoing sentence by providing Customer with access to features and functions of the Services such that Customer can fulfill the Data Subject Request without assistance from Wasabi. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Wasabi shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Wasabi is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from Wasabi's provision of such assistance.

## 7. CONFIDENTIALITY.

**7.1.** **Wasabi's Personnel.** Unless otherwise required by law, Wasabi shall keep and maintain all Personal Data in strict confidence, using such a degree of care as is appropriate to avoid unauthorized access, use or disclosure (taking into account the state of the art, costs and implementation, and the nature, scope, context, and purposes of the Processing as well as the risks to the rights of Data Subjects). Unless otherwise required by Applicable Law, Wasabi shall not disclose or permit access to the Personal Data other than to its employees, officers, directors, attorneys, and agents who need to know or access the Personal Data to meet Wasabi's obligations under this DPA and the Services Agreement (each, a "**Wasabi Representative**"). Wasabi shall require that such Wasabi Representatives: (a) are informed of the confidential nature and use restrictions regarding the Personal Data; and (b) have committed themselves to maintaining the confidentiality of the Personal Data or are under an appropriate statutory obligation of confidentiality.

## 8. SECURITY MEASURES.

**8.1.** **Security Requirements.** Wasabi shall implement reasonable and appropriate technical, physical, and organizational measures designed to adequately safeguard and protect against a Security Incident (each, a "**Security Measure**") as further set forth in Appendix C. Without limiting the foregoing, Wasabi shall ensure that all such Security Measures comply with all Data Protection Laws as well as the terms and conditions of the Services Agreement.

**8.2.** **Security Testing.** Wasabi shall regularly test, assess, and evaluate the effectiveness of its Security Measures.

## 9. SECURITY INCIDENTS.

**9.1.** **Notification of a Security Incidents.** In the event of a Security Incident, Wasabi will notify Customer without undue delay after becoming aware of the Security Incident, but in no event later than any periods required by applicable Data Protection Laws or described in the Services Agreement. Wasabi shall, as part of the notification provided under this Section 9.1 and to the extent reasonably available at the time of notice, provide all information required under applicable Data Protection Laws. Wasabi shall update Customer as additional relevant information set forth in the foregoing sentence becomes available without further undue delay.

**9.2. Maintaining Security Incident Documentation.** Wasabi shall maintain and preserve applicable documents, records, and other data reasonably related to any Security Incident.

**9.3. No Admission of Fault.** Notwithstanding anything to the contrary, in no event will any notice of a Security Incident under this Section 9 be construed as an acknowledgement of Wasabi of any fault or liability of Wasabi with respect to any Security Incident.

## 10. SUBPROCESSORS.

**10.1. Use of Subprocessors.** Wasabi may use Subprocessors to perform the Processing pursuant to this Data Processing Agreement. The name and contact information, together with details of the processing to be performed, will be as set forth in Appendix D, as amended by Wasabi from time to time subject to the terms of this Section 10.

**10.2. Subprocessors.** To the extent permitted under applicable Data Protection Laws and subject to Wasabi's compliance with the remainder of this Section 10, Customer hereby provides a general authorization for Wasabi to engage Subprocessors to Process Personal Data in connection with the provision of the Service.

**10.3. New or Changed Subprocessors.** Wasabi shall provide reasonable notification to Customer where Wasabi wishes to engage a new Subprocessor to Process Personal Data. Customer shall have five (5) days after issuance of such notice to notify Wasabi in writing of any objections on reasonable grounds.

**10.4. Subprocessor Requirements.** Wasabi shall ensure that all Subprocessors so engaged are bound by written agreements with terms and conditions at least as restrictive as the relevant terms and conditions contained in this DPA. Wasabi shall remain fully liable to the Customer for a Subprocessors failure to fulfil its obligations under such agreement.

**11. RIGHTS OF THOSE AFFECTED BY PROCESSING.** The applicable Data Subjects are the intended third-party beneficiaries of this DPA. In this regard, Data Subjects shall be entitled to exercise all rights available to Customer under this DPA, and enforce all terms and conditions of this DPA to the extent such rights, terms, and conditions impact or otherwise relate to the Processing of such Data Subjects' Personal Data. Each Party shall use reasonable efforts to support the other affected Party in their efforts to safeguard these rights.

**12. COMPELLED DISCLOSURES.** Any disclosure by Wasabi or its representatives of any of the Personal Data pursuant to applicable federal, state, or local law, regulation, or valid order issued by a court or governmental agency of competent jurisdiction (a "**Legal Order**") will be subject to the terms of this Section 12. Prior to making such a disclosure, Wasabi shall, to the extent permitted under the Legal Order, make commercially reasonable efforts to provide Customer with: (a) prompt written notice of the disclosure requirements set forth in the Legal Order so that Customer may seek, at its sole cost and expense, a protective order or other remedy; and (b) reasonable assistance, at Customer's sole cost and expense, in opposing such disclosure or seeking a protective order or other limitations on disclosure. If, after providing such notice and assistance as required herein, Wasabi remains subject to a Legal Order to disclose any Personal Data, Wasabi shall, upon Customer's request, use commercially reasonable efforts to obtain assurances from the applicable court or agency that such Personal Data will be Processed solely to the extent necessary and otherwise remain confidential.

## 13. CROSS-BORDER TRANSFERS OF PERSONAL DATA.

**13.1. Prohibited Transfers.** Neither Customer nor Wasabi shall transfer any Personal Data to another country unless the transfer complies with the Data Protection Laws.

**13.2. Permitted Countries for Processing; Cross-Border Data Transfer Restrictions.** Appendix B lists all of the countries Wasabi may receive, access, transfer, or store Personal Data. Wasabi must not Process (including through Subprocessors) the Personal Data outside the countries listed on Appendix B without Customer's prior written consent. If applicable Data Protection Laws restricts cross-border Personal Data transfers from certain countries (each such country, an "**Export Restricted Country**"), each Party shall only transfer that Personal Data to the other Party, a Party's Affiliate, or a Subprocessor under the following conditions, as applicable: (a) the recipient of the Personal Data (the "**Data Importer**"), either through its location or participation in a valid cross-border transfer mechanism under the Data Protection Laws, as identified in Appendix B, may legally receive that Personal Data; (b) the transferor of the Personal Data (the "**Data Exporter**") obtained valid Data Subject consent to the transfer, to the extent necessary or permitted under the Data Protection Laws; or (c) the transfer otherwise complies with or is otherwise permitted under the Data Protection Laws.

**13.3. Essential Equivalence.** The Parties shall assess, taking into account the circumstances of the transfer, whether the level of protection for Personal Data afforded by the Applicable Laws that are applicable to the Data Importer are essentially equivalent to that provided under the Data Protection Laws applicable to the Data Exporter. In the event either Party believes, in its reasonable discretion, that it is unable to comply with the requirements under the applicable cross-border transfer mechanism specified in Appendix B (and any regulations promulgated thereunder, each as amended, supplemented or otherwise modified from time to time in accordance with Applicable Law) or provide such a level of protection to Personal Data, such Party shall notify the other Party of such determination and the Customer may, if it agrees with such determination and the Parties cannot reasonably supplement the cross-border transfer mechanism described in Appendix B with additional terms and conditions that would provide the required level of protection or adopt another cross-border data transfer mechanism that will provide the required level of protection, suspend any further transfers of Personal Data or terminate the Services Agreement.

**13.4. Standard Contractual Clauses.** If any Personal Data transfer between Wasabi and Customer requires or otherwise utilizes the execution of the applicable Standard Contractual Clauses in order to comply with the applicable Data Protection Laws, the Parties hereby execute such Standard Contractual Clauses contained in Exhibit 1 and contained in Exhibit 2 as completed as set forth herein, and take all other actions required to legitimize the transfer, including, as necessary: (a) formally executing the applicable Standard Contractual Clauses with a written or electronic signature, as necessary; (b) co-operating to register the Standard Contractual Clauses with any supervisory authority in any applicable country; (c) procuring approval from any such supervisory authority; and (d) providing additional information about the transfer to such supervisory authority.

## 14. TERM AND TERMINATION.

**14.1. Term.** The term of this DPA will commence on the Effective Date and will remain in force until the earliest date that: (a) this DPA is replaced or repealed by mutual agreement of Customer and Wasabi; (b) this DPA is replaced by an alternative agreement in order to meet additional or changed rights and obligations under Data Protection Laws; or (c) the Services Agreement is terminated or expires (the "**Term**").

**14.2. Survival.** In the event Wasabi retains Personal Data after the Term for any reason, Wasabi shall continue to comply with the confidentiality and privacy obligations hereunder until it is no longer in possession of Personal Data, and such obligations shall survive past the Term of this Data Processing Agreement until such time that Processor and all of its Subprocessors no longer Process such Personal Data. In addition, any provision of this DPA that expressly or by implication should come into or continue in force on or after such period described in the foregoing sentence in order to protect Personal Data will remain in full force and effect.

**14.3. Changes in Data Protection Laws.** If a change in any of the Data Protection Laws prevents either Party from fulfilling all or part of its obligations under the Services Agreement or this DPA, the Parties shall negotiate a change to this DPA, the Services, or the Services Agreement in good faith and shall suspend the Processing of Personal Data until that Processing complies with the new requirements. If the Parties are unable to bring the Processing of Personal Data into compliance with the Data Protection Laws within a reasonable period, they may terminate the Services Agreement upon written notice to the other Party.

## 15. PERSONAL DATA RETURN AND DESTRUCTION.

**15.1. Return or Destroy Personal Data.** The Services include certain features and functions that allow Customer to delete or obtain a copy of all Personal Information Processed by Wasabi for Customer. Upon a reasonable time after the termination or expiration of this Data Processing Agreement for any reason as set forth in the Services Agreement: (a) Wasabi shall, and shall require all Subprocessors to, cease Processing Personal Data except as otherwise set forth hereunder; and (b) Wasabi shall, and shall require all Subprocessors to, securely destroy all or any Personal Data related to this agreement in its possession or control.

**15.2. Retention of Data on Backup; Retention Required by Law.** Notwithstanding the foregoing, to the extent it is not commercially reasonable for Wasabi or its Subprocessors to remove Personal Data from archive or other backup media, Wasabi may retain Personal Data on such media in accordance with its backup or other disaster recovery procedures. If any Applicable Law or Legal Order requires Wasabi to retain any Personal Data that Wasabi would otherwise be required to return or destroy, it shall notify Customer in writing of that retention requirement, giving details of the Personal Data that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

## 16. RECORDS; AUDITS.

**16.1. Records.** Wasabi shall keep, and shall require its Subprocessors to keep, reasonably detailed, accurate, and up-to-date books, records, and other documents (including computer files) regarding any Processing of Personal Data it carries out for Customer, including but not limited to, the access, control, and security of the Personal Data, approved Subprocessors and Affiliates, the Processing purposes, and any other records required by the applicable Data Protection Law (collectively, the "**Records**"). Such Records shall be maintained during the Term and, unless Data Protection Law requires a longer retention period, for a period of at least ninety (90) days after the Term.

**16.2. Demonstrating Compliance.** Upon Customer's request, Wasabi shall make available to Customer Records and other information as necessary to demonstrate Wasabi's (and its Subprocessors') material compliance with this DPA and any applicable Data Protection Laws.

**16.3. Self Audits.** At least once per year, Wasabi will conduct audits of its Personal Data Processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this DPA.

**16.4. Audit Reports.** Wasabi shall retain an independent third-party auditing firm to perform an annual audit of Wasabi's Processing of Personal Data. Upon Customer's written request and Customer's execution of Wasabi's standard confidentiality agreement, Wasabi will make the relevant results of such audit available to Customer for review. Customer will treat such audit reports as Wasabi's confidential information and subject to Wasabi's standard confidentiality agreement.

**16.5.** **Customer Audits.** Customer shall have the right to request or mandate an audit by instructing Wasabi to carry out an audit described in 16.3 or 16.4, provided that no such audit has been requested by Customer or performed by Wasabi in the past twelve (12) month period. If Wasabi declines to follow any such instruction requested by Customer regarding audits, including inspections, Customer may terminate the Services Agreement in accordance with its terms.

## 17. MISCELLANEOUS.

**17.1.** **Amendment.** This Data Processing Agreement may not be amended or modified except in writing signed by authorized representatives of both Parties.

**17.2.** **Severability.** If any provision in this Data Processing Agreement is determined to be ineffective or void by any court or body of competent jurisdiction or by virtue of any legislation to which it is subject, it shall be ineffective or void to that extent only and the validity and enforceability of the remaining provisions of the Data Processing Agreement and the Services Agreement shall not be affected. The Parties shall promptly and in good faith replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. The Parties shall similarly promptly and in good faith add any necessary appropriate provision where such a provision is found to be missing by any court or body of competent jurisdiction or by virtue of any legislation to which this Data Processing Agreement is subject.

**17.3.** **Governing Law.** This Data Processing Agreement shall be governed by and construed in accordance with law that governs the Services Agreement.

**17.4.** **Headings.** The headings in this Data Processing Agreement are for reference only and shall not affect the interpretation of this Data Processing Agreement.

[Remainder of page intentionally left blank]

## Schedule A

## Data Processing Purposes and Details

1. **Nature of the Processing.** Data storage and such other Services as initiated by Customer from time to time.

2. **Purposes of the Processing.** The purpose of the data processing under this DPA is the provision of data storage and such other Services initiated by Customer from time to time.

3. **Categories of Data Subjects.** The data subjects may include Customer's customers, employees, vendors, and end users.

4. **Categories of Personal Data.** Categories of personal data include any personal data uploaded by Customer.

5. **Sensitive Data Processed (if any).** The data processed is determined by customer. Sensitive data will be processed if uploaded by Customer. Only the categories of sensitive data uploaded by customer will be processed.

6. **Duration of Processing.** The duration of the processing is determined by the Customer.

7. **Frequency of Processing.** Data will continue to be stored until deleted by customer or deleted as a result of account termination.

## Appendix B

## Countries of Processing and Legal Basis for Transfers

| Country | Lawful Basis for Processing |
|---|---|
| United States of America | ☐ Located in a country within the EU/EEA or Switzerland<br>☐ Located within a country with a current determination of adequacy (including UK).<br>☒ Standard Contractual Clauses<br>☐ Binding Corporate Rules<br>☐ Other (describe in detail): ________________________________________ |
| | |

## Appendix C

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

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

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Security Policies and Procedures applicable to the specific Services purchased by data exporter, and accessible https://wasabi.com/security-policy or otherwise made reasonably available by data importer. Data Importer will not materially decrease the overall security of the Services during a subscription term.

## Appendix D

## List of Subprocessors

Please refer to https://wasabi.com/legal/sub-processors/

**Exhibit 1**

## STANDARD CONTRACTUAL CLAUSES

**(Controller – Processor)**

**(Only for Processing of Data Subjects in the European Economic Area, not in the United Kingdom)**

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

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

*Clause 4.*

**Interpretation**

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

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

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

*Clause 5.*

**Hierarchy**

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

*Clause 6.*

**Description of the transfer(s)**

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

## *Clause 7.*

## 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[2] (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

### 8.9. Documentation and compliance.

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

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

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

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

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

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

*Clause 9.*

### Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects[(3)]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

*Clause 10.*

### Data subject rights

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

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

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

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

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

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

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

### *Clause 14.*

### Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination including those requiring the disclosure of data to public authorities or authorising access by such authorities relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as

(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 (c), 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

part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

(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 paragraph (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) paragraph (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 (a) 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

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

## *Clause 18.*

### Choice of forum and jurisdiction

(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 1

**Data exporter(s):**

1. Name: *As noted in the applicable Wasabi account holder information.*

   Address: *As noted in the applicable Wasabi account holder information.*

   Contact person’s name, position and contact details: *As noted in the applicable Wasabi account holder information.*

   Activities relevant to the data transferred under these Clauses: *Data storage*

   Signature and date: *Electronically signed*

   Role (controller/processor): *Controller*

**Data importer(s):**

1. Name: *Wasabi Technologies LLC*

   Address: *111 Huntington Ave., Suite 2900; Boston, MA 02199*

   Contact person’s name, position and contact details: *Legal Department, 1-617-307-7912, privacy@wasabi.com*

   Activities relevant to the data transferred under these Clauses: *Uploading data to be stored and downloading stored data*

   Signature and date: *Electronically signed*

   Role (controller/processor): *Processor*

### A. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

*The data subjects may include Customer’s customers, employees, vendors, and end users.*

Categories of personal data transferred

*Categories of personal data include any personal data uploaded by Customer.*

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 data processed is determined by customer. Sensitive data will be processed if uploaded by Customer. Only the categories of sensitive data uploaded by customer will be processed.*

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

*Data will continue to be stored until deleted by customer or deleted as a result of account termination.*

Nature of the processing:

*Data storage and such other Services as initiated by Customer from time to time.*

Purpose(s) of the data transfer and further processing:

*The purpose of the data processing under this DPA is the provision of data storage and such other Services initiated by Customer from time to time.*

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

*Personal data will be retained for as long as directed by Customer, or for legitimate backup and legal compliance purposes, as described above.*

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

*As noted in Appendix D of this Data Processing Agreement*

## B. **COMPETENT SUPERVISORY AUTHORITY**

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

Ireland

*ANNEX II*

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

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

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Security Policies and Procedures applicable to the specific Services purchased by data exporter, and accessible https://wasabi.com/security-policy or otherwise made reasonably available by data importer. Data Importer will not materially decrease the overall security of the Services during a subscription term.

*ANNEX III*

## LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. *As noted in Appendix D of this Data Processing Agreement*

## Exhibit 2

## Standard Contractual Clauses (processors)

## (Only for Processing of Data Subjects in the UK)

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

Name of the data exporting organisation: *As noted in the applicable Wasabi account holder information*

Address: *As noted in the applicable Wasabi account holder information*

Tel.: ..................................................; fax:...................................; e-mail:....................................

Other information needed to identify the organisation:

…………………………………………………………

(the data **exporter**)

And

Name of the data importing organisation: *Wasabi Technologies LLC*

Address: *111 Huntington Ave., Suite 2900; Boston, MA 02199*

Tel.: *1-617-307-7912*; fax:...................... ; e-mail: *privacy@wasabi.com*

Other information needed to identify the organisation:

………………………………………………………………

(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 *'Commissioner'* shall have the same meaning as in the UK GDPR;

(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 covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 UK;

(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 subprocessor 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 subprocessor 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 Commissioner) and does not violate the applicable data protection law;

(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 covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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*[5]

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 Commissioner 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 by the data exporter, where applicable, in agreement with the Commissioner;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

[5] 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.

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

(j) to send promptly a copy of any subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor 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 Commissioner;

   (b) to refer the dispute to the UK courts.

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 Commissioner if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 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 country of the United Kingdom in which the data exporter is established, namely …………………………………………………………………………….

*Clause 10*

### *Variation of the contract*

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11*

### *Subprocessing*

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[6]. Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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

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

by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing 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 Commissioner.

### *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 subprocessor 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 subprocessor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter:**
Name (written out in full): *As noted in the applicable Wasabi account holder information.*
Position: *As noted in the applicable Wasabi account holder information.*
Address: *As noted in the applicable Wasabi account holder information.*
Other information necessary in order for the contract to be binding (if any):

Signature *Signed electronically*

(stamp of organisation)

**On behalf of the data importer:**
Name (written out in full): *Wasabi Technologies LLC*
Position:
Address: *111 Huntington Ave., Suite 2900; Boston, MA 02199*
Other information necessary in order for the contract to be binding (if any):

Signature *Signed electronically*

(stamp of organisation)

## APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

**Data exporter**
The data exporter is (please specify briefly your activities relevant to the transfer):
*Uploading data of its selection.*

**Data importer**
The data importer is (please specify briefly activities relevant to the transfer):
*Providing Data storage and such other Services as initiated by Customer from time to time.*

**Data subjects**
The personal data transferred concern the following categories of data subjects (please specify):
*The data subjects may include Customer's customers, employees, vendors, and end users.*

**Categories of data**
The personal data transferred concern the following categories of data (please specify):
*Categories of personal data include any personal data uploaded by Customer.*

**Special categories of data (if appropriate)**
The personal data transferred concern the following special categories of data (please specify):
*The data processed is determined by customer. Special categories of data will be processed if uploaded by Customer. Only the categories of data uploaded by customer will be processed.*

**Processing operations**
The personal data transferred will be subject to the following basic processing activities (please specify):
*Data storage.*

DATA EXPORTER
Name: *The Customer executing this Data Processing Agreement*
Authorised Signature *Signed electronically*

DATA IMPORTER
Name: *Wasabi Technologies LLC*
Authorised Signature *Signed electronically*

## 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):**

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Security Policies and Procedures applicable to the specific Services purchased by data exporter, and accessible https://wasabi.com/security-policy or otherwise made reasonably available by data importer. Data Importer will not materially decrease the overall security of the Services during a subscription term.