DATA PROCESSING AGREEMENT

This Data Processing Agreement, including any attachments, exhibits or schedules (collectively the "**DPA**") is incorporated into and made a part of the Wasabi Technologies Customer Agreement governing the provision of Services (the "**Services Agreement**") entered into by Customer ("**Customer**") and Wasabi Technologies LLC ("**Wasabi**"). In the event of conflict, the provisions of this DPA shall control over the Services Agreement. Customer and Wasabi may be referred to individually as a "**Party**" or collectively as the "**Parties**."

DEFINITIONS. Capitalized terms used in this DPA without definition have the meanings assigned in the Services Agreement.

"**Affiliate**" means any corporation, partnership or other entity now existing or hereafter organized that directly or indirectly controls, is controlled by or under common control with such party. For purposes of this definition "control" means the direct possession of a majority of the outstanding voting securities of an entity.

"**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.

"**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 all worldwide data protection and privacy laws and regulations applicable to the processing of Personal Data under this DPA, including, where applicable and without limitation: (a) GDPR; (b) UK GDPR; (c) CCPA; and, (d) 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 Schedule D, as amended, supplemented or otherwise modified from time to time.

"**GDPR**" means the EU General Data Protection Regulation (EU Regulation 2016/679) 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.

"**Security Incident**" means any accidental, unlawful, or unauthorized use, modification, loss, compromise, destruction, or disclosure of, or access to, Personal Data processed by Wasabi on behalf of Customer. For the avoidance of doubt, "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.

"**UK GDPR**" means the United Kingdom Data Protection Act of 2018 and the United Kingdom General Data Protection Regulation, 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 United Kingdom's International Data Transfer Addendum to the Standard Contractual Clauses, as may be amended, modified, or replaced by the United Kingdom, a completed copy of which comprises Schedule E, as amended, supplemented or otherwise modified from time to time.

The terms "**Controller**", "**Data Subjects**", "**Member State**", "**Processor**", "**Process**", "**Processing**", "**Personal Data**", "**Personal Information**" and "**Sub-processor**" have the meanings given to them in Data Protection Laws, as applicable, and include any equivalent or corresponding terms applied by such Data Protection Laws. If and to the extent that Data Protection Laws do not define such terms, then the definitions given in GDPR will apply.

SCOPE AND ROLES.

This DPA applies to the extent Wasabi processes Customer Personal Data subject to applicable Data Protection Laws in connection with the Services. In this context, Customer is the Controller under applicable Data Protection Law and Wasabi is the Processor, except where Customer is the Processor under applicable Data Protection Law, Wasabi shall be the Sub-processor. Customer remains in full control of what data it uploads to the Services and where such data is stored.

CUSTOMER OBLIGATIONS.

Customer will comply with all Data Protection Laws required of it to perform its obligations under this DPA and is responsible for: (i) providing any notices or obtaining any consents required in order to process the Personal Data; (ii) making an independent determination as to whether the technical and organisational measures for the Services meet Customer's requirements; and (iii) ensuring Customer's instructions to Wasabi for the processing of Personal Data comply with Data Protection Laws. Customer will be solely responsible for the accuracy, quality, and legality of, and the means by which, Customer acquired the Personal Data.

WASABI'S OBLIGATIONS.

Wasabi will comply with all Data Protection Laws required to perform its obligations under this DPA and will only process the Personal Data pursuant to Customer's instructions as set forth in this DPA. The details of the processing operations Wasabi will conduct on behalf of the Customer are specified in Schedule A (Data Processing Purposes and Details).

CONFIDENTIALITY.

Wasabi will not collect, retain, use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Data outside of the direct business relationship with Customer for the benefit of anyone other than Customer. Wasabi personnel having access to the Personal Data, if any, will be (a) informed of the confidential nature and use restrictions regarding the Personal Data; and (b) subject to an appropriate statutory or contractual obligation of confidentiality. Notwithstanding the foregoing, and for the avoidance of doubt, Wasabi may use and disclose Personal Data as follows to the extent permitted by applicable Data Protection Laws: (i) to provide and support the Service; (ii) to build or improve the Service, provided 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; (iii) to detect Security Incidents, or to protect against fraudulent or illegal activity; (iv) as otherwise explicitly permitted under Data Protection Law; (v) to respond to any Legal Order; and (vi) as Customer otherwise consents in writing.

DOCUMENTED INSTRUCTIONS.

Wasabi and Wasabi personnel having access to Personal Data, if any, will only Process the Personal Data pursuant to Customer's documented instructions. Customer agrees that this DPA together with the Services Agreement constitute the documented instructions. To the extent permitted by applicable law, Wasabi shall promptly notify Customer if, in its reasonable opinion, Customer's instruction do not comply with Data Protection Laws.

In the event Wasabi is required under any applicable law to Process the Personal Data in excess of Customer's documented instructions, Wasabi will promptly notify Customer of such requirement, unless such applicable law prohibits such notification, in which case Wasabi will notify Customer as soon as the applicable law permits it to do so.

Wasabi will promptly inform Customer in the event Wasabi can no longer comply with this DPA, in which case, Customer may immediately suspend any Processing of Personal Data and/or terminate the Services pursuant to the Services Agreement.

ASSISTANCE IN COMPLIANCE WITH OBLIGATIONS UNDER DATA PROTECTION LAWS.

Taking into account the limited nature of Wasabi's Processing and the information available to it, Wasabi will provide reasonable assistance to Customer in meeting Customer's obligations under Data Protection Laws, including responding to requests from Data Subjects or government or regulatory bodies. Wasabi reserves the right to invoice, and Customer agrees to pay, for any material costs arising from Wasabi's provision of such assistance. As between the Parties, Customer is solely responsible for communicating directly with Data Subjects.

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 herein.

SECURITY MEASURES.

Wasabi will maintain reasonable and appropriate technical, physical, and organisational measures designed to adequately safeguard and protect against a Security Incident (each, a "**Security Measure**") as further set forth in Schedule B. Wasabi will regularly test, assess, and evaluate the effectiveness of its Security Measures.

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 will, as part of the notification provided under this Section, and to the extent reasonably available at the time of notice, provide all information required under applicable Data Protection Laws.

Wasabi will maintain and preserve relevant documents, records, and other data reasonably related to any Security Incident. Notwithstanding anything to the contrary, in no event will any notice of a Security Incident under this Section be construed as an acknowledgement of Wasabi of any fault or liability of Wasabi with respect to any Security Incident.

SUB-PROCESSORS.

Wasabi may use Sub-processors to perform the Processing pursuant to this DPA. The name and contact information, together with details of the processing to be performed, will be as set forth in Schedule C, as amended by Wasabi from time to time subject to the terms of this Section.

To the extent permitted under applicable Data Protection Laws, Customer hereby authorizes the use of all Sub-processors identified in Schedule C and provides a general authorization for Wasabi to engage Sub-processors to Process Personal Data in connection with the provision of the Service.

Wasabi will provide reasonable notification to Customer where Wasabi wishes to engage a new Sub-processor and Customer will have thirty (30) days after issuance of such notice to notify Wasabi in writing of any objections on reasonable grounds.

Wasabi will ensure that all Sub-processors it engages are bound by written agreements with terms and conditions at least as restrictive as those contained in this DPA. Wasabi will remain responsible to Customer for a Sub-processor's failure to fulfil its obligations under such agreement.

COMPELLED DISCLOSURES.

In the event Wasabi receives a valid order issued by a court or governmental agency of competent jurisdiction (a "**Legal Order**"), Wasabi will first attempt to redirect the Legal Order to the Customer to the extent that Wasabi is permitted to do so by the terms of the Legal Order or as a matter of law. If unsuccessful, Wasabi will, to the extent permitted by such Legal Order, make commercially reasonable efforts to provide Customer with: (a) prompt written notice of the disclosure requirements set forth in the Legal Order prior to disclosure 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 will 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.

CROSS-BORDER TRANSFERS OF PERSONAL DATA.

Customer is responsible for deciding the storage region where the Content it uploads to the Service should be stored. Wasabi will not transfer that Content to another location, except as set forth in the Services Agreement. Notwithstanding the foregoing, Wasabi may access or process Personal Data from countries other than the selected storage region, as set forth in this DPA, which may constitute a data transfer. Wasabi may Process (including through Sub-processors) the Personal Data in the countries identified in the list of Sub-processors referenced in Schedule C (including all applicable appendices). Customer is responsible for making an independent determination that any such transfer complies with or is otherwise permitted under the Data Protection Laws. Wasabi will, if so requested by Customer, provide reasonable assistance to Customer in performing a transfer impact assessment.

To the extent that any such transfer is governed by the GDPR or the UK GDRP, the Parties are deemed to have executed such Standard Contractual Clauses attached hereto, as applicable. Additionally, Customer may, if it so desires, electronically execute and download a copy of the Standard Contractual Clauses.

CCPA AND CPRA.

To the extent that the CCPA and/or the CPRA apply to Wasabi's processing of Personal Data, Customer and Wasabi agree that Wasabi is acting as a Service Provider, strictly for the purpose of providing and supporting the Services as set forth in the Service Agreements, or as otherwise permitted by the CCPA and/or the CPRA.

TERM AND TERMINATION.

This DPA will remain in place and govern Wasabi's Processing activities until such time as Wasabi no longer provides Services to Customer, unless this DPA is terminated or replaced before such time. In the event Wasabi retains Personal Data after the Services Agreements is terminated or expires for any reason, Wasabi will continue to comply with the confidentiality and privacy obligations hereunder until it is no longer in possession of 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. 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 will negotiate a change to this DPA, the Services, or the Services Agreement in good faith and will 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.

PERSONAL DATA RETURN AND DESTRUCTION.

The Services include certain features and functions that allow Customer to delete, export or copy all of the data uploaded by Customer to the Service at any time during the Term of the Services Agreement. Thereafter, Wasabi will, and will require its Sub-processors to: (a) stop Processing Personal Data except as otherwise set forth herein;

and (b) securely destroy all or any Personal Data related to this agreement in its possession or control, which includes deleting Customer's account, after which time Customer will no longer have access to the data uploaded.

Notwithstanding the foregoing, to the extent it is not commercially reasonable for Wasabi or its Sub-processors 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.

RECORDS AND AUDITS.

Wasabi will keep, and will require its Sub-processors 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 Sub-processors and Affiliates, the Processing purposes, and any other records required by the applicable Data Protection Law (collectively, the "**Records**"). Such Records will be maintained during the Term and, unless Data Protection Law requires a longer retention period, for a period of at least ninety (90) days thereafter.

Upon Customer's request, not more than once every 12 (twelve) months, Wasabi will make available to Customer Records and other information as necessary, in Wasabi's sole discretion, to demonstrate Wasabi's (and its Sub-processors') material compliance with this DPA and any applicable Data Protection Laws. If Customer reasonably believes, after review of such Records, that Wasabi or its Sub-processors are not in material compliance with this DPA and any applicable Data Protection Laws, then Customer may request one follow up audit, to be conducted at a time and place as determined by Wasabi, whereby additional detail will be provided to address any reasonable concerns raised.

MISCELLANEOUS.

1. **Amendment.** This DPA may not be amended or modified except in writing signed by authorized representatives of both Parties.
2. **Severability.** If any provision in this DPA 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 DPA 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 such provision. The Parties shall similarly promptly and in good faith add any necessary or appropriate provision if 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 DPA is subject.
3. **Governing Law.** This DPA shall be governed by and construed in accordance with law that governs the Services Agreement.

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, as further set forth in the Services Agreement.

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, as further set forth in the Services Agreement.

3. **Categories of Data Subjects.** Depending on Customer's use of the Services, which are unknown to Wasabi, the data subjects may include Customer's customers, employees, vendors, and end users.

4. **Categories of Personal Data.** Depending on Customer's use of the Services, which are unknown to Wasabi, the categories of personal data may include without limitation, contact information such as name, email address, phone number or address, location data such as IP addresses, personal information, such as marital status, gender and birth date, authentication data such as passwords, audio and video, financial data.

5. **Sensitive Data Processed (if any).** The Customer determines the Personal Data to be uploaded to the Services, including Sensitive Personal Data. Only the categories of Sensitive Personal Data uploaded by customer will be processed.

6. **Duration of Processing.** The duration of the processing is continual, until Services are no longer provided in accordance with clauses 15 and 16 of this DPA.

7. **Frequency of Processing.** Data will continue to be stored until deleted by customer or deleted as a result of account termination in accordance with clauses 15 and 16 of this DPA.

Schedule B

TECHNICAL AND ORGANISATIONAL MEASURES

Wasabi maintains administrative, physical, and technical measures designed to protect Customer Content (as such term is defined in the Services Agreement) uploaded to the Services, as well as Personal Data that may be contained therein, as detailed below in this Schedule B. Wasabi may modify or change such measures and related policies at its discretion, but will not materially decrease the overall security of the Services during a subscription term.

1. Policies; Business Continuity

Wasabi maintains formal, documented policies concerning information security and compliance. Summary copies of such policies are available upon request, subject to Wasabi's discretion. Wasabi policies address items such as prohibition of unauthorized information transfer, denial of service protection, resource availability, boundary protection, transmission confidentiality and integrity, cryptographic key management and cryptographic protection, public key infrastructure certs, and protection of data in transit and at rest. Wasabi requires all Wasabi employees to comply with its information security policies and procedures.

Wasabi's Business Continuity Plan (BCP) is designed to ensure the continued operation of business-critical systems in the event of a natural or man-made disaster, interruption, or essential changes. Wasabi's BCP is structured around recovery teams with specific responsibilities, including disaster management, operations, network, facilities, and communications. Wasabi performs internal risk assessments at least annually, with a Risk Assessment Report provided to executive staff and the Board of Directors. Wasabi is assessed by certain third-party auditors on an annual basis. Wasabi routinely scans for outside vulnerabilities and potential issues with internal code.

2. Physical Security

The Wasabi cloud storage Service is hosted in top-tier data center facilities that are secure, redundant, and certified in accordance with industry-standard compliance protocols such as SOC 2 and ISO 27001. Sites are staffed 24/7/365 with on-site security personnel to protect against unauthorized entry. Security cameras continuously monitor the facility outdoors, indoors and into the Wasabi server cages. Biometric readers and two-factor or greater authentication mechanisms are designed to secure Wasabi server cage access. Wasabi staff must have a data center access card, and accessing the server cage room and cage requires both an access card and biometric identification (e.g. fingerprint reader). Visitors must be registered in advance and escorted by a data center badge holder.

Entry to Wasabi's physical office headquarters location can only be gained via a personnel badge. Visitors must be pre-registered and escorted by Wasabi personnel while in the office space.

3. Network Architecture and Security

Wasabi employs advanced network security elements, including firewalls and other boundary protection devices to monitor and control communications at internal and external network borders. These border security devices segregate customers and regulate the flow of communications between networks in a manner designed to prevent unauthorized access to Wasabi infrastructure and services. Wasabi periodically scans for outside vulnerabilities.

An intrusion detection system (IDS) is used for IDS-related incidents. Network defense and host intrusion prevention systems are monitored daily by Wasabi's Operations Team. If tests or monitors fail, the Wasabi

Operations Team is automatically notified. Wasabi provides a firewall with ACL rules and private subnet services with ACL. Firewall protection is managed over SSH, and firewall policies are deny-all-allow-by-exception by default. Internal network segmentation is used to further isolate sensitive production resources. Wasabi's servers, DNS servers and network devices such as firewalls, routers, and switches are protected using relevant hardening practices.

Due to the security concerns posed to Wasabi and its customers, Wasabi does not permit customers to test the security status of network devices that Wasabi owns, operates or that are located in a data center used by Wasabi. Further, Wasabi does not permit denial-of-service, flooding, or any similar test activity that involves significant consumption of network bandwidth.

4. Encryption

Wasabi encrypts data at rest and in transmission unless otherwise specified in specific product terms and conditions. All data at rest is encrypted using 256-bit AES. Data in transmission is encrypted using the HTTPS protocol. Customers using third-party tools to interact with Wasabi should contact their developer to confirm the tools' compliance with HTTPS. Wasabi utilizes TLS 1.2 and in certain circumstances TLS 1.3, with the exception that any public bucket created by a customer resolves to a TLS 1.0 security protocol. This is under the control of the customer and can be mitigated by not creating public buckets. Wasabi also uses the cryptographic protection encryption algorithm SHA-256.1.

Wasabi supports server-side encryption (SSE). The SSE options include SSE-S3 (using AES256 encryption - X-Amz-Server-Side-Encryption: AES256) and SSE-C (customer-based key - X-Amz-Server-Side-Encryption-Customer-Key). Customers can specify the SSE parameters using a S3 client application when writing objects to buckets. With the encryption key a customer provides as part of their request, Wasabi manages the encryption as it writes to disks and decryption when customers access their objects. Customers must manage the encryption keys they provide. An access key is for use with third-party applications and is used to make programmatic calls to AWS API actions. Customers must use two types of access keys: Access Key ID and Secret Access Key. Wasabi does not access or view a customer's secret key as part of providing the Service. A customer's Access Key ID is visible to support staff when logging in.

5. Data Access and Integrity

Wasabi does not access or view customer Content as part of providing the Service. As a result, it is the customer's responsibility to ensure their data maintains its accuracy and integrity. Wasabi may view certain metadata associated with customer data (e.g. filenames) as part of providing or supporting the Service. Wasabi offers user authentication features to permit tightly controlled access to stored data. Administratively defined policies can selectively grant read/write and administrative permissions to users, groups of users, and roles. Wasabi cloud storage Services are designed to provide eleven 9s object durability and offer customers an optional data immutability capability. Customers can sign up for Direct Connect options to help prevent being exposed to the public internet when transferring and receiving data.

6. System Information Backup; Customer Data Replication

Wasabi has a strategy of real-time continuous backup of system information. Every database server has 2 backups that are in sync with the primary.

Customers can choose to replicate their data to another Wasabi storage region using the object replication feature. Customers can restrict access to their data using Identity and Access Management (IAM) policies that specify the users that can access specific buckets and objects. IAM policies provide a programmatic way to manage S3 permissions for multiple users.

7. Customer Users & Passwords

Customers are responsible for creating and managing their authorized users and access/encryption keys. A user is an individual for whom a customer creates Wasabi authentication, giving that person permission to perform actions in Wasabi. Users must authenticate using a username and password. Customer Root Users can choose to implement Multi-Factor Authentication. Customers can implement roles and policies to restrict user access to information, including Administrator Access, Full Access, Write, Read Only, and Billing access permissions. All passwords are hashed while stored and encrypted in transmission. Shared accounts are not supported.

8. Event Logging

Wasabi customers are notified of planned maintenance and unplanned service interruptions via https://status.wasabi.com. The status webpage also maintains a history of incidents. Customers can subscribe to status updates for one or more storage regions. Bucket logs and administrative logs can be activated by the customer and, upon activation, are stored in the customer bucket.

9. Certifications and Audits

Wasabi undergoes an annual Type 2 HIPAA/HITECH audit and a CyberGRX assessment. Wasabi has completed audits for SEC SEA Rule 17a-4, FINRA, and SOX. Customers may obtain Data Center SOC 2 and ISO 27001 compliance certificates upon request, and under conditions set by Wasabi. Wasabi's immutability functionality (object lock with compliance mode) is designed to fulfill certain requirements relevant to electronic storage, including in the following regulations: Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), which regulates exchange members, brokers or dealers; Financial Industry Regulatory Authority (FINRA) Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f); and Commodity Futures Trading Commission (CFTC) in 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

10. Training

All Wasabi personnel receive security awareness training relevant to their role and responsibilities. Training is conducted upon hire, with periodic refresher and spot training and simulations. All employees receive periodic HIPAA Awareness Training, and those responsible for implementing Wasabi's HIPAA Compliance program also complete HIPAA Security Training. Wasabi staff that have access to the production environment and the CJIS Administrator receive periodic CJIS Level IV Awareness Training. Training is documented for all employees.

11. Data Retention

Wasabi's Record Retention and Destruction Policy is designed to ensure that necessary records and documents are adequately maintained and that records no longer needed by Wasabi or of no value are appropriately discarded. Wasabi's customer agreement, partner agreements, addendums, and other contract documents further detail the parties' rights and obligations with respect to retention of customer data. Customer data is retained so long as the account remains active and in good standing, subject to the terms of the customer agreement and Wasabi policy or as otherwise required by law. Data generally cannot be retrieved once the account has terminated or expired. Any customer data that requires destruction is sanitized per methodologies consistent with the most current version of NIST Special Publication 800-88. Customers who have terminated their account may request a Certificate of Sanitation by contacting compliance@wasabi.com. Unneeded or

outdated Wasabi internal records are destroyed either systematically (such as through periodic purging of email), or by disposing of outdated documents and records as they are observed in files.

12. System Access

The level of security assigned to an internal Wasabi user to the Wasabi information systems is based on the principle of least privilege, granting the minimum access required to carry out legitimate job responsibilities assigned to a user's job classification. Segregation of duties is in place to help ensure the separation between the requesting, approving, and granting of system access. Access requests are tracked via tickets. Access to Wasabi information systems and applications requires a login ID and password that is unique to each Wasabi workforce member. Password characters are replaced with asterisks when typed. Passwords must include at least eight characters and can be reset by the user at any time. In addition, the Wasabi IT Department can change, or require a change, of the user's password. In the event of employee termination, access is disabled within 24 hours.

13. Supply Chain Risk Management

Wasabi has established processes, procedures and tools used to manage third party risk within its supply chain. This includes due diligence review of third- party suppliers' security practices, including, where appropriate, questionnaires, SOC 2, ISO 27001, and/or other audit reports, and contract documentation. Additionally, Wasabi uses contractual measures to mandate third-party compliance, including acknowledgment of Wasabi's vendor Code of Conduct.

Schedule C

LIST OF SUB-PROCESSORS

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

Schedule D

STANDARD CONTRACTUAL CLAUSES

(Controller – Processor) and

(Processor – Sub-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

[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.

pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3.

Third-party beneficiaries

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

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

(ii) Clause 8 - Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

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

Module Two: Transfer Controller to Processor

8.1. Instructions.

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

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

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

8.3. Transparency. On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

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

8.5. Duration of processing and erasure or return of data.

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete

all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6. Security of processing.

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

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

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

8.7. Sensitive data.

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely

identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8. Onward transfers.

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[(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.

Module Three: Transfer Processor to Sub-processor

8.1 Instructions

[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.

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[3].

[3] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

[4] 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 purposes of these Clauses.

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

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

Clause 9.

Use of sub-processors

Module Two: Transfer Controller to Processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 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[5]. The Parties agree that, by complying with this Clause, the data

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

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.

Module Three: Transfer Processor to Sub-processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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.[6] 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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.

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

Clause 10.

Data subject rights

Module Two: Transfer Controller to Processor

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

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

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

Module Three: Transfer Processor to Sub-processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11.

Redress

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

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

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

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

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

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

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

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

Clause 12.

Liability

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

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

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

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

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

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

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

Clause 13.

Supervision

(a) [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[7];

(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.

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

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

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

Clause 15.

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

15.1. Notification.

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

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

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

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

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

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

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

15.2. Review of legality and data minimisation.

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

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

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

SECTION IV – FINAL PROVISIONS

Clause 16.

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion

of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17.

Governing law

(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 I

A. LIST OF PARTIES

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 (or Processor, where applicable)

Data importer(s):

1. Name: Wasabi Technologies LLC

   Address: 75 Arlington St., Suite 810; Boston, MA 02116

   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 (or Sub-processor, where Customer is a Processor)

B. DESCRIPTION OF TRANSFER

As set forth in Schedule A to the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

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

Ireland

Annex II

TECHNICAL AND ORGANISATIONAL MEASURES

See Schedule B to the DPA.

Annex III

LIST OF SUB-PROCESSORS

See Schedule C to the DPA.

Schedule E

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: *As noted in the applicable Wasabi account holder information.* Trading name (if different): Main address (if a company registered address): *As noted in the applicable Wasabi account holder information.* Official registration number (if any) (company number or similar identifier):	Full legal name: Wasabi Technologies LLC Trading name (if different): Main address (if a company registered address): 75 Arlington St., Suite 810, Boston, MA 02116 Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email: *As noted in the applicable Wasabi account holder information.*	Full Name (optional): Job Title: Legal Department Contact details including email: privacy@wasabi.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

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

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	X	X		General Authorisation	30 days	
3						
4						

Table 3: Appendix Information

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

Annex IA: List of Parties: Annex I
Annex IB: Description of Transfer: Annex I
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Schedule B
Annex III: List of Sub processors (Modules 2 and 3 only): Schedule C

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.