Data Processing Agreement (DPA)

This Data Processing Agreement including its Attachments ("**DPA**") between CAKE Software, Inc. ("**Vendor**") and the entity that receives any Vendor Products from Vendor (the "**Customer**") pursuant to a written or electronic agreement which governs the provision of those Vendor Products (the "**Agreement**") shall apply to the extent that (i) Vendor Processes Personal Data on behalf of the Customer, and (ii) either the Agreement expressly incorporates this DPA by reference or the parties sign this DPA.

This DPA is supplemental to, and forms an integral part of, the Agreement and is effective upon the earlier of signature or its incorporation into the Agreement, which incorporation may be specified in the Agreement or an executed amendment to the Agreement. In case of any conflict or inconsistency between the terms of the Agreement and this DPA, this DPA shall take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

The term of this DPA shall follow the Term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

1. Definitions

"*California Personal Information*" means Personal Data that is subject to the CCPA.

"*Canadian Privacy Laws*" means the data protection laws applicable in Canada and/or its provinces, in each case as hereinafter amended, supersede, or replaced, including:

(i) The Personal Information Protection and Electronic Documents Act of 2000 ("**PIPEDA**");

(ii) In Quebec: the Act to Modernize Legislative Provisions As Regards the Protection of Personal Information, also known as Bill 64, and the Act Respecting the Protection of Personal Information in the Private Sector, CQLR P-39.1, which is amended thereby (collectively "**Bill 64**");

(iii) In Alberta: the Personal Information Protection Act [of Alberta] ("**PIPA Alberta**"); and

(iv) In British Columbia: the Personal Information Protection Act [of British Columbia] ("**PIPA BC**").

"*Consumer,*" "*Business,*" "*Sell*" and "*Service Provider*" shall have the meanings given to them in the CCPA.

"*Controller*" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"*Data Protection Laws*" means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws, US Data Privacy Laws, and Canadian Data Privacy Laws; in each case to the extent applicable and as amended, repealed, consolidated or replaced from time to time.

"*Data Subject*" means the individual to whom Personal Data relates.

"*European Data*" means Personal Data that is subject to European Data Protection Laws.

"*European Data Protection Laws*" means data protection laws applicable in the European Union, the European Economic Area ("**EEA**") and/or their member states, Switzerland and the United Kingdom, in each case as hereinafter amended, superseded, or replaced, including:

(i) Regulation 2016/679 of the European Parliament and of the Council 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) ("**GDPR**");

(ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC;

(iii) Applicable national implementations of (i) and (ii); the Data Protection Act of 2018; and GDPR as it forms part of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (collectively "*UK GDPR*"); and

(iv) Swiss Federal Act on Data Protection of 19 June 1992 (as amended 25 September 2020) and its Ordinance ("*FADP*").

"*Instructions*" means the written, documented instructions issued by Customer to Vendor and directing the same to perform a specific or general action with regard to Personal Data.

"*Onward Transfer*" means a transfer of Personal Data from a third-party, such as a Processor, to a fourth-party, such as a Sub-Processor, or beyond.

"*Permitted Affiliates*" means any of Customer's Affiliates (as defined under the Agreement):

(i) That are permitted to use the Products pursuant to the Agreement, but have not signed their own separate agreement with Vendor;

(ii) For whom Vendor Processes Personal Data; and

(iii) That are subject to Data Protection Laws.

"*Personal Data*" means any information provided by or collected on behalf of Customer relating to an identified or identifiable individual where such information is protected under applicable Data Protection Laws as personal data, personal information, personally identifiable information, or any equivalent thereof.

"*Personal Data Breach*" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Vendor and/or its Sub-Processors in connection with the provision of the Products. "Personal Data Breach" shall not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"*Processing*" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms "Process", "Processes" and "Processed" will be construed accordingly.

"*Processor*" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

"*Products*" means the goods and services provided by Vendor to Customer under the Agreement.

"*Standard Contractual Clauses*" or "**SCCs**" means, for the processing of Personal Data that is subject to the GDPR, the standard contractual clauses approved pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021, as available at http://data.europa.eu/eli/dec_impl/2021/914/oj, as they may be amended, superseded, or replaced. For the Processing of Personal Data that is subject to the UK GDPR, the Standard Contractual Clauses also include the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/, as it may be amended, superseded, or replaced (the "**UK Addendum**").

"*Sub-Processor*" means any third-party engaged by Vendor to carry out specific Processing activities in accordance with the Instructions and subject to further limitations set forth in this DPA.

"***Third Country***" means, for the Processing of Personal Data that is subject to the GDPR, UK GDPR, or FADP, a country that is not a member of the EEA, United Kingdom, or Switzerland, respectively, and not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws).

"***US Privacy Laws***" means the data protection laws applicable in the United States of America and/or its states, in each case as hereinafter amended, supersede, or replaced, including:

(i) In **California**: the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (the "**CCPA**");

(ii) In **Colorado**: the Colorado Privacy Act (the "**CoPA**");

(iii) In **Connecticut**: the Connecticut Personal Data Privacy and Online Monitoring Act (the "**CPDP**");

(iv) In **Utah**: the Utah Consumer Privacy Act, which goes into effect on December 31, 2023 (the "**UCPA**"); and

(v) In **Virginia**: the Virginia Consumer Data Protection Act (the "**VCDPA**").

2. **Roles of the Parties**

a. Under European Data Protection Laws. With respect to European Data that is Processed under this DPA, the parties acknowledge and agree that Vendor is a Processor and Customer is either (i) a Controller, or (ii) a Processor acting on behalf of a Controller that is not a party to the Agreement or this DPA.

b. Under the CCPA. With respect to California Personal Information, the parties acknowledge and agree that Customer is a Business and Vendor is a Service Provider.

c. Under US Privacy Laws, except the CCPA. With respect to Personal Data that is Processed under this DPA and governed by US Privacy Laws except the CCPA, the parties acknowledge and agree that Vendor is a Processor and Customer is either (i) a Controller, or (ii) a Processor acting on behalf of a Controller that is not a party to the Agreement or this DPA

d. Under Canadian Privacy Laws. With respect to Personal Data that is Processed under this DPA and governed by Canadian Privacy Laws, the parties acknowledge and agree that (i) Vendor Processes Personal Data on behalf of Customer and assumes the obligations under applicable Canadian Privacy Laws that apply to that role, and (ii) Customer, through its Instructions to Vendor, determines the purposes and means of the Processing of Personal Data and assumes the obligations under applicable Canadian Privacy Laws that apply that role.

3. **Customer Responsibilities**

a. Compliance with Laws. With respect to the Personal Data that Vendor collects from or on behalf of Customer, Customer shall be responsible for complying with all its obligations under applicable Data Protection Laws and shall inform Vendor without undue delay if it is not able to comply with its responsibilities under this sub-section (a) or applicable Data Protection Laws. In particular but without prejudice to the generality of the foregoing, Customer acknowledges and agrees that it shall be solely responsible for:

(i) the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data;

(ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by Customer for marketing purposes);

(iii) ensuring it has the right to transfer, or provide access to, the Personal Data to Vendor for Processing in accordance with the terms of the Agreement (including this DPA);

(iv) ensuring that its Instructions to Vendor regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and

(v) complying with all laws (including Data Protection Laws) applicable to any content created, sent or managed through the Products, including those relating to obtaining consents (where required) to send communications, the content of the communications, and its communication deployment practices.

b. Instructions. The parties agree that the following constitutes Customer's complete and final Instructions to Vendor in relation to the Processing of Personal Data: (i) the terms of the Agreement and this DPA, including the Attachments hereto, (ii) direction from Customer through its use of the Products in accordance with the Agreement, and (iii) this general authorization by Customer which hereby permits Vendor to use Personal Data for any business operations incident to providing the Products to Customer. Additional instructions outside the scope of the Instructions must be agreed to according to the process for amending the Agreement or this DPA, where applicable.

c. Security. Customer is responsible for independently determining whether the data security provided for in the Products adequately meets its obligations under applicable Data Protection Laws. Customer is also responsible for its secure use of the Products, including protecting account access to the Products and the security of Personal Data in transit to and from the Products (including the secure backup or encryption of any such Personal Data).

4. Vendor Obligations

a. Compliance with Instructions. Vendor shall only Process Personal Data for the purposes described in this DPA, including Attachment 1, or as otherwise agreed within the scope of Customer's lawful Instructions, except where and to the extent otherwise required by applicable law. Vendor is not responsible for compliance with any Data Protection Laws applicable to Customer or Customer's industry that are not generally applicable to Vendor.

b. Conflict of Laws. If Vendor becomes aware that it can no longer meet its obligations under the applicable Data Protection Laws or Process Personal Data in accordance with Customer's Instructions due to a legal requirement under any applicable law, Vendor will:

(i) promptly notify Customer of that legal requirement to the extent permitted by the applicable law; and

(ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as Customer issues new Instructions with which Vendor is able to comply. If this provision is invoked, Vendor will not be liable to Customer under the Agreement for any failure to provide the applicable Products until such time as Customer issues new lawful Instructions with regard to the Processing.

c. Technical and Organizational Measures. Vendor shall implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under Attachment 2 (*Technical and Organizational Measures*) to this DPA. Notwithstanding any provision to the contrary, Vendor may modify or update the contents of Attachment 2 at its discretion provided that such modification or update does not result in a material degradation in the technical and organizational measures set forth therein.

d. Confidentiality. Vendor shall ensure that any personnel whom Vendor authorizes to Process Personal Data on its behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

e. Personal Data Breaches. Vendor will notify Customer without undue delay after it becomes aware of any Personal Data Breach and shall provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by Customer. At Customer's request, Vendor will promptly provide Customer with such reasonable assistance as necessary to enable Customer to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Customer is required to do so under Data Protection Laws.

f. Deletion or Return of Personal Data. Vendor will delete or return all Personal Data (including copies thereof) Processed pursuant to this DPA on termination or expiration of the Products in accordance with the procedures and timeframes set out in the Agreement, save that this requirement shall not apply to the extent Vendor is required by applicable law to retain some or all of the Personal Data, or to Personal Data that Vendor has archived on back-up systems, which data Vendor shall securely isolate and protect from any further Processing and delete in accordance with its deletion practices.

g. Demonstration of Compliance. Vendor shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections by Customer, in order to assess compliance with this DPA. Customer acknowledges and agrees that it shall exercise its audit and inspection rights under this DPA by instructing Vendor to supply, on a confidential basis, (i) a summary copy of an independently validated report of its security programs (e.g. SOC 2, Type II Report), along with copies of any related policies and other documentation, or its hosting provider's security programs and related policies and documentation if Vendor does not host the Personal Data itself, or (ii) if Vendor does not have such a report, written responses to all reasonable requests for information made by Customer necessary to confirm Vendor's compliance with this DPA, along with copies of any related policies and other documentation. Customer shall not exercise this right to audit and inspect more than once per calendar year.

5. Data Subject Requests

Where required by applicable Data Protection Laws, Vendor shall implement measures that it can use to assist Customer with its obligations under Data Protection Laws, including Customer's obligation to respond to requests from data protection authorities or Data Subjects that seek to exercise their rights under applicable Data Protection Laws ("***Data Subject Requests***"). All Data Subject Requests must provide sufficient information to verify the identity of the Data Subject.

To the extent that Customer is unable to independently address a Data Subject Request through the Products, then upon Customer's written request Vendor shall provide reasonable assistance to Customer to respond to any Data Subject Requests. Customer shall reimburse Vendor for the commercially reasonable costs arising from this assistance.

If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to Vendor, Vendor will, to the extent that Vendor can identify Customer as the source of the Personal Data in question through its standard due diligence processes, promptly inform Customer and will advise the Data Subject to submit their request to Customer. Customer shall be solely responsible for responding substantively to any such Data Subject Requests and all other communications with Data Subjects that relate to Personal Data.

6. Data Protection Assessments

To the extent required by applicable law, Vendor will provide reasonable assistance to Customer to enable Customer to conduct and document data protection assessments, provided that the required information is reasonably available to Vendor, and Customer does not otherwise have access to the required information.

7. Sub-Processors

Customer agrees that Vendor may engage Sub-Processors to Process Personal Data on Customer's behalf. Customer hereby approves, as Sub-Processors, the entities on its list of Sub-Processors located below. Any desired changes to the list of Sub-Processors must follow the amendment process set forth in Section 11(a) of this DPA.

Where Vendor engages Sub-Processors, Vendor will execute a written agreement with any Sub-Processor that imposes data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors. Vendor will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause Vendor to breach any of its obligations under this DPA.

The list of approved Sub-Processors is as follows:

Entity	Country of Origin	Purpose
Adobe, Inc.	USA	Contract Generation
Amazon Web Services, Inc.	USA	Cloud Infrastructure Hosting
Atlassian Corporation Plc	USA	Customer Record Retention
Freshworks, Inc.	USA	Customer Service/ Support
Gong.io, Inc.	USA	Call Note Taking/ Sales Coaching

Hubspot, Inc.	USA	Automated Marketing/ Communication
Perseus Group Software Corp.	Canada	Back Office Support (Accounting & Finance)
Perseus Management Group, Inc.	USA	Back Office Support (Legal, Accounting, Finance, and HR) and Shared IT Services (email, word processing, etc.)
Salesforce, Inc.	USA	Customer Relationship Management
Salesloft, Inc.	USA	Sales/ Marketing
Slack Technologies, Inc.	USA	Internal & Client Communication

8. International Processing

Customer acknowledges and agrees that Vendor may Process Personal Data on a global basis as necessary to provide the Products in accordance with the Agreement. Vendor shall ensure such transfers are made in compliance with the requirements of applicable Data Protection Laws.

9. Additional Provisions for European Data

a. Scope. This Section 9 (Additional Provisions for European Data) shall apply only with respect to European Data. In the event that the terms and conditions in this Section 9 conflict with those in the other sections of this DPA, the terms and conditions in this Section 9 shall take precedence

b. Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent required by European Data Protection Laws, Vendor will provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities, provided that the required information is reasonably available to Vendor, and Customer does not otherwise have access to the required information.

c. Transfer Mechanisms for Cross Border Transfers.

(i) Vendor shall not transfer, or permit any of its Sub-Processors to transfer, European Data to any Third Country, unless it first takes all such measures as are necessary to ensure the transfer will be made in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that has (A) a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, (B) achieved binding corporate rules authorization in accordance with European Data Protection Laws, or (C) executed appropriate standard contractual clauses as adopted or approved in accordance with applicable European Data Protection Laws and conducted any requisite data transfer impact assessments in conjunction therewith.

(ii) The Standard Contractual Clauses will apply if, and only to the extent that, Personal Data is transferred, either directly or via Onward Transfer, to any Third Country, (each a "***Cross Border Transfer***").

(A) With respect to Cross Border Transfers from the EEA or Switzerland to a Third Country, the iteration of the Standard Contractual Clauses set forth in Part 1 (EEA/Swiss Transfers) of Attachment 3 shall apply.

(B) With respect to Cross Border Transfers from the United Kingdom to a Third Country, the iteration of the Standard Contractual Clauses set forth in Part 2 (UK Transfers) of Attachment 3 shall apply.

(iii) Notwithstanding Section 9(c)(ii), the Standard Contractual Clauses will not apply to a Cross Border Transfer if Vendor has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Cross Border Transfers.

(iv) If and to the extent the Standard Contractual Clauses (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict.

10. Additional Provisions for California Personal Information

a. Scope. This Section 10 (Additional Provisions for California Personal Information) shall apply only with respect to California Personal Information. In the event that the terms and conditions in this Section 10 conflict with those in the other sections of this DPA, the terms and conditions in this Section 10 shall take precedence.

b. Responsibilities. The parties agree that Vendor will process California Personal Information as a Service Provider strictly for the purposes set forth in Attachment 1 of this DPA (the "***Business Purpose***") and as otherwise permitted by the CCPA.

(i) Vendor shall not:

(A) combine the California Personal Information that the Vendor receives from, or on behalf of, the Customer with California Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, provided that the Vendor may combine California Personal Information to perform any business purpose permitted under the CCPA, and may also aggregate, deidentify, or anonymize California Personal Information so it no longer meets the California Personal Information definition, and may use such aggregated, deidentified, or anonymized data for its own research and development purposes or for any other purpose that is not prohibited under the CCPA;

(B) attempt to or actually re-identify any previously aggregated, deidentified, or anonymized data and will contractually prohibit downstream data recipients from attempting to or actually re-identifying such data;

(C) sell California Personal Information (as defined in the CCPA);

(D) retain, use, or disclose California Personal Information for any purpose other than for the Business Purpose or as otherwise permitted by the CCPA; or

(E) retain, use, or disclose California Personal Information outside of the direct business relationship between Customer and Vendor.

(ii) Vendor shall:

(A) comply with all applicable obligations imposed by the CCPA;

(B) provide the same level of privacy protection as is required by the Customer under the CCPA;

(C) promptly comply with any Customer request or instruction requiring the Vendor to provide, amend, transfer, or delete California Personal Information, or to stop, mitigate, or remedy any unauthorized processing;

(D) permit the Customer to take reasonable and appropriate steps to stop and remediate unauthorized use of California Personal Information; and

(E) notify Customer immediately if it receives any complaint, notice, or communication that directly or indirectly relates either party's compliance with the CCPA; specifically, the Vendor must notify the Customer within seven (7) business days if it receives a verifiable consumer request under the CCPA.

c. Certification. Vendor certifies that it understands and will comply with the restrictions set out in Section 10(b) (Responsibilities).

11. General Provisions

a. Amendments. Notwithstanding anything else to the contrary in the Agreement and without prejudice to Section 4(a) (Compliance with Instructions), or Section 4(c) (Security), Vendor reserves the right to make any updates and changes to this DPA or list of Sub-Processors, and that any such modifications become effective thirty (30) days after the date that Vendor either (1) notifies Customer that the updated DPA or list of Sub-Processors has been posted to a particular URL, or

(2) distributes the updated DPA or list of Sub-Processors to any known point-of-contact for Customer. Customer is responsible for reviewing and becoming familiar with the updated DPA or list of Sub-Processors. If, prior to the effective date of the updated DPA or list of Sub-Processors, Customer notifies Vendor of its objection to any modification of the DPA or list of Sub-Processors, then Vendor shall either (i) negotiate with Customer in good faith to resolve any such objection, or (ii) upon thirty (30) days' notice to Customer, terminate the DPA and any portion of the Agreement that governs Products which are dependent upon its execution. If Vendor exercises its right to terminate pursuant to the terms of this Section, Customer shall be entitled to a pro-rata refund of any Fees already paid by Customer for the affected Products, calculated from the effective date of any such termination.

b. Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

c. Limitation of Liability. Each party's liability, and where applicable, each of Customer's Affiliates' liability, taken in aggregate, arising out of or related to this DPA, including the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, shall be subject to the limitations and exclusions of liability set out in the Agreement. In no event shall either party's liability be limited with respect to any individual Data Subject's data protection rights under this DPA(including the Standard Contractual Clauses) or otherwise.

d. Governing Law. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

12. Parties to this DPA

a. Permitted Affiliates. Customer enters into this DPA (including, where applicable, the Standard Contractual Clauses) on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Permitted Affiliates, thereby establishing a separate DPA between Vendor and each such Permitted Affiliate. Each Permitted Affiliate agrees to be bound by the obligations under this DPA. For the purposes of this DPA only, the term "Customer" shall include Customer and such Permitted Affiliates.

b. Authorization. The legal entity entering into this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

c. Remedies. Except where applicable Data Protection Laws require a Permitted Affiliate to exercise a right or seek any remedy under this DPA against Vendor directly by itself, the parties agree that: (i) solely the Customer entity that is the contracting party to the Agreement shall exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all communication with Vendor under the DPA and shall be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.

Attachment 1 - Details of Processing
This Attachment forms part of the DPA.

A. Nature and Purpose of Processing
Vendor will Process Personal Data as necessary to provide the Products pursuant to the Agreement, as further specified in an Order Form or SOW, and as further instructed by Customer through its use of the Products.

B. Duration of Processing
Subject to the "Deletion or Return of Personal Data" section of this DPA, Vendor will Process Personal Data for the duration of the Agreement only, unless otherwise agreed in writing.

C. Categories of Data subjects
Customer may provide Personal Data relating to the following categories of Data Subjects to Vendor in the course of using the Products, or incident to the use thereof, the extent of which is determined and controlled by Customer in its sole discretion:

Customer's employees, contractors, collaborators, customers, partners, prospects, suppliers and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to Customer's end users.

D. Categories of Personal Data
Customer may provide the following categories of Personal Data to Vendor in the course of using the Products, or incident to the use thereof, the extent of which is determined and controlled by Customer in its sole discretion:
  - Contact Information (e.g. name, address, telephone number, email address, etc).
  - Financial and payment data (e.g. credit card number, bank account, transactions)
  - Device identifiers and internet or electronic network activity (IP addresses, GAID/IDFA, browsing history, timestamps, etc.)

E. Special categories of data (if appropriate)
The parties do not anticipate Processing special categories of Personal Data or sensitive personal information, as those terms are defined under applicable Data Privacy Laws.

F. Processing operations
Personal Data will be Processed in accordance with the Agreement and this DPA and may be subject to the following Processing activities:

a. Storage and other Processing necessary to provide, maintain and improve the Products provided to Customer; and/or

b. Disclosure in accordance with the Agreement, this DPA, and/or as compelled by applicable laws.

Attachment 2 – Technical and Organizational Measures

This Attachment forms part of the DPA. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

Vendor currently observes the technical and organizational measures described in this Attachment 2 to ensure an appropriate level of Personal Data protection, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of the Data Subjects.

1. Security Management	Vendor maintains a written information security program (ISP) that includes policies, processes and controls governing the processing of Personal Data, designed to (a) secure Personal Data against accidental or unlawful loss, access or disclosure; (b) identify reasonably foreseeable risks to security and unauthorized access to Vendor Network, and (c) minimize security risks, including through risk assessment and regular testing. For the purpose of this Schedule, "**Vendor Network**" means the Vendor's data center facilities, servers, networking equipment, assets and hosting software and systems as employed or used by the Vendor to process or store Personal Data.
2. Maintaining of an Information Security Policy	Vendor established, maintains and follows an ISP that is based on its security and privacy policies that are regularly reviewed and disseminated to all relevant parties and personnel within the organization. Security policies and derived procedures clearly define information security responsibilities, including responsibilities for: • Maintaining security policies and procedures; • Secure development (if applicable), operation and maintenance of software and systems; • Security alerts and incidents response procedures (including escalation); • User account administration; • Monitoring and control of all systems that may have access to Personal Data.
3. Secure Networks and Systems	To protect Personal Data, Vendor has installed and maintains a firewall (or functionally equivalent technology) that controls all traffic allowed between Vendor Network and any untrusted networks or devices, as well as traffic into and out of more sensitive assets within it's the Vendor Network. This includes current documentation, change control and regular reviews.
4. Personal Data Protection Measures (including storage limitation, data minimization and retention and encryption)	• Vendor limits Personal Data storage to the minimum necessary for the provision of the service and implements applicable data retention and disposal policies. • Vendor uses industry standard encryption for all stored Personal Data, except for Internet Protocol (IP) addresses, which are only encrypted in transit. • Vendor has documented and implemented all necessary procedures to protect cryptographic keys used to secure stored Personal Data against misuse. • All transmission of Personal Data across open, public networks is encrypted using industry standard encryption algorithms.
5. Vulnerability Management Efforts	Vendor protects its systems against malware, including via installation of anti-virus software (or similar programs), which is regularly updated. Vendor further maintains secure systems and applications by: • Establishing and evolving processes to identify and fix security vulnerabilities; • Implementing strict change procedures for changes to system components, including separation of development and test

	environments from production environments and avoiding use of Personal Data for testing or development; • If Vendor is a software developer, facilitating a secure software development process based on best practices, that incorporates information security throughout the software-development lifecycle;
6. Access Control Measures	• Vendor restricts access to Personal Data on a need-to-know basis to ensure access is limited to authorized personnel and for the purposes agreed in this DPA. This is achieved by: • Establishing and maintaining access control system(s) for systems that process Personal Data, with a default "deny-all" setting. • Management of access to such systems using individually assigned unique IDs, which allow identification and authentication and ensures that actions taken on Personal Data can be traced and reviewed. • Implementing processes that control the addition, deletion, modification, revocation and disabling of credentials and user permissions, as well as lock out of users after repeated failed access attempts and timely termination of idling session. • For user authentication purposes, utilizes strong passwords that meet industry standard complexity rules, and are changed on a regular basis.
7. Restriction of Physical Access to Personal Data Processing Systems	• Physical components of the Vendor Network are housed in nondescript facilities. Physical barrier controls are used to prevent unauthorized entrance to such facilities. Passage through the physical barriers requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel. • Any physical access to systems that process Personal Data is restricted using appropriate entry controls and procedures that distinguishes between onsite personnel and visitors. • Access to sensitive areas is controlled and includes processes for authorization based on job function. • Media and backups are secured and their (internal and external) distribution is controlled. Media containing Personal Data that is no longer needed for business or legal reasons is rendered unrecoverable or physically destroyed.
8. Regular Monitoring and Testing of Networks	• Access to Vendor Network and Personal Data is monitored using mechanisms that allow tracking, alerting, and analysis on a regular basis as well as upon need. • All systems that process Personal Data are provided with correct and consistent time and audit trails, including file-integrity monitoring to prevent change of existing log data and/or generate alerts in such case. Audit trails for critical systems are kept for, at least, one year. • Security of such systems is regularly tested and reviewed at least annually. This is to ensure that security controls for system components, processes and custom software continue to reflect a changing environment. Security testing includes: • Processes to test rogue wireless access points, • Internal and external network vulnerability tests that are carried out at least annually. An external, qualified party carries out the external network vulnerability tests. • External and internal penetration tests using Vendor's penetration test methodology that is based on industry-accepted penetration testing approaches that cover the all systems that process Personal Data and cover application-layer as well as network-layer tests

	• Test results are kept on record and findings are remediated in a timely manner. • Use of IDS (intrusion detection system) and file-integrity monitoring in daily operations to detect and alert against network intrusions and unauthorized modification or access.
9. Incident Response Plan	• Vendor has implemented and maintains an incident response plan and is prepared to respond immediately to a system breach. Such plan includes: • Definition of roles, responsibilities, and communication and contact strategies in the event of a compromise, including notifications to customer; • Specific incident response procedures; • Analysis of legal requirements for reporting compromises; • Regular review and testing of the plan; • Incident management personnel that is available 24/7; • Training of staff; • Vendor established and maintains a business continuity process (BCP). • Data backup processes have been implemented and are tested regularly.
10. Third Party Risk Management Program	Prior to engaging new third-party service providers or vendors who will have access to customer Data or systems that process Personal Data, Vendor conducts an established due diligence process, that includes an assessment of the service provider data security practices.

Attachment 3

Part 1 – EEA/Swiss Transfers

1) The parties agree that the terms of the Standard Contractual Clauses, as supplemented by this Part 1, are hereby incorporated by reference and shall apply to the transfer of Personal Data from the EEA or Switzerland to Third Countries.

2) Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the transfer of Personal Data to a Third Country is effectuated by Customer as the Controller of the Personal Data and Vendor is the Processor of the Personal Data.

3) Module Three (Processor to Processor) of the Standard Contractual Clauses shall apply where the transfer of Personal Data to a Third Country is effectuated by Customer as the Processor of the Personal Data and Vendor is a Sub-Processor of the Personal Data.

4) The parties acknowledge that the Standard Contractual Clauses solicit input from the parties in several clauses, and the parties agree that the following responses shall apply (to Module Two and Module Three, where applicable):

   a) Clause 7 of the SCCs shall not be applicable.

   b) In Clause 9(a), Option 2 (general written authorisation) shall apply, the time period for prior notice of Sub-Processor changes shall be thirty (30) days.

   c) In Clause 11, the optional language will not apply, and Data Subjects shall not be able to lodge a complaint with an independent dispute resolution body.

   d) In Clause 17, option 1 shall apply. The Parties agree that the Standard Contractual Clauses shall be governed by the laws of the Republic of Ireland.

   e) In Clause 18(b), the parties choose the courts of the Republic of Ireland as their choice of forum and jurisdiction.

5) Annex I.A of the SCCs shall be completed as follows (for Module Two and Module Three):

   a) "**Data Exporter**":

   i) **Name:** The entity identified as "Customer" in the DPA

   ii) **Address:** The address for Customer associated with its account or as otherwise specified in the DPA or Agreement.

   iii) **Contact person's name, position and contact details:** The contact details associated with Customer's account, or as otherwise specified in the DPA or the Agreement.

   iv) **Activities relevant to the data transferred under these Clauses:** The activities specified in Attachment 1 of the DPA.

   v) **Role (controller/processor):** With respect to Module Two, Controller; with respect to Module Three, Processor.

   b) "**Data Importer**":

   i) **Name:** Cake Software, Inc.

   ii) **Address:** 11350 McCormick Road, EP3, Suite 200, Hunt Valley, Maryland, 21031, United States of America

iii) **Contact person's name, position and contact details:** Santi Pierini, President – Digital Marketing, santi.pierini@getcake.com

iv) **Activities relevant to the data transferred under these Clauses:** The activities specified in Attachment 1 of the DPA.

v) **Role (controller/processor):** With respect to Module Two, Processor; with respect to Module Three, Processor.

c) <u>Signature and Date</u>: By entering into the DPA, data exporter and data importer are deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the DPA.

6) Annex I.B of the SCCs shall be completed as follows (for Module Two and Module Three):

a) **Categories of data subjects whose personal data is transferred:** Categories of data subjects are specified in Attachment 1 of the DPA.

b) **Categories of personal data transferred:** The personal data is described in Attachment 1 of the DPA.

c) **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 exporter will transfer the sensitive Personal Data listed in Section E of Attachment 1 to the DPA (if any). To the extent that data importer receives sensitive Personal Data, data importer will apply those restrictions or safeguards that are necessary and appropriate based on applicable Data Protection Laws.

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

e) **Nature of the processing:** The nature of the processing is described in Attachment 1 of the DPA.

f) **Purpose(s) of the data transfer and further processing:** The purpose of the processing is described in Attachment 1 of the DPA.

g) **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 the later of (i) the date upon which data exporter asks data importer to delete or destroy the Personal Data in accordance with the terms of the DPA or the Agreement, and (ii) as long as permitted by applicable Data Protection Laws.

h) **For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing:** The subject matter, nature and duration of the processing are described in Attachment 1 of the DPA.

7) **Annex I.C** of the SCCs shall be completed as follows: The competent supervisory authority in accordance with Clause 13 of the Standard Contractual Clauses is the supervisory authority in the Member State stipulated in Section 4(d) of this Attachment 3.

8) Attachment 2 to this DPA (Technical and Organizational Measures) serves as **Annex II** of the SCCs.

9) Section 7 of this DPA (Sub-Processors) serves as **Annex III** of the SCCs.

Part 2- UK Transfers

1) The parties agree that the terms of the Standard Contractual Clauses, as supplemented by Part 1 above and amended by the iteration of the UK Addendum attached hereto as <u>Exhibit 1 to Attachment 3</u> of this DPA, are hereby incorporated by reference and shall apply to the transfer of Personal Data from the United Kingdom to Third Countries. The Standard Contractual Clauses, together with the UK Addendum, which are deemed to be amended to the extent necessary to enable them to: (a) lawfully facilitate transfers by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to such transfers; and (b) provide appropriate safeguards for the transfer in accordance with Articles 46 of the UK GDPR.

2) This Part 2 shall (a) be read and interpreted in the light of the provisions of UK GDPR and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 of the UK GDPR, and (b) not be interpreted in a way that conflicts with rights and obligations provided for in the UK GDPR.

3) Any references to legislation, including the UK Addendum, mean that legislation, as may be amended from time to time (including consolidation, reenactment or replacement of such legislation following the Effective Date of this DPA).

4) To the extent there is any conflict between the Standard Contractual Clauses, together with the UK Addendum, and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses, together with the UK Addendum, will prevail.

Exhibit 1 to Attachment 3 – International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

Part 1: Tables

Table 1: Parties

Start date	Upon the effective date of the DPA.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: As stated in Part I, Section 5(a) of Attachment 3 to the DPA Trading name (if different): Main address (if a company registered address): As stated in Part I, Section 5(a) of Attachment 3 to the DPA Official registration number (if any) (company number or similar identifier):	Full legal name: As stated in Part I, Section 5(b) of Attachment 3 to the DPA Trading name (if different): Main address (if a company registered address): As stated in Part I, Section 5(b) of Attachment 3 to the DPA Official registration number (if any) (company number or similar identifier):
Key Contact	As stated in Part I, Section 5(a) of Attachment 3 to the DPA	As stated in Part I, Section 5(b) of Attachment 3 to the DPA
Signature (if required for the purposes of Section 2)	NOT REQUIRED	NOT REQUIRED

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: June 4, 2021 template, effective on the Start Date listed above Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

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

Table 3: Appendix Information

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

Annex 1A: List of Parties: As stated in Part I, Section 5 of Attachment 3 to the DPA

Annex 1B: Description of Transfer: As stated in Part I, Section 6 of Attachment 3 to the DPA

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As stated in Part I, Section 8 of Attachment 3 to the DPA

Annex III: List of Sub processors (Modules 2 and 3 only): As stated in Part I, Section 9 of Attachment 3 to the DPA

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 16: ☒ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

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