Customer Data Processing Addendum

This Data Processing Addendum ("**DPA**") provides a set of supplemental obligations that **Memcyco** (defined below) hereby assumes as part of the agreement (the "**Agreement**") with each Memcyco customer (the "**Customer**") who has purchased and maintains an active subscription to use Memcyco's software as a service (SAAS) products (the "**SAAS Products**"). This DPA shall be effective with regard to each such Customer on the effective date of the Agreement with such Customer ("Effective Date"). This DPA shall apply solely with regard to the processing by Memcyco and its Sub-processors of the Customer Personal Data of data subjects who are covered under the then-current GDPR and/or the California Privacy Statutes (defined below).

In the event that Memcyco and Customer have entered into a separate signed agreement or addendum with regard to compliance with the GDPR, this DPA shall not apply; provided, that at a minimum, Memcyco shall in any case be bound by its obligations set forth in this DPA.

1. **Definitions.** All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

"**Affiliate**" has the meaning set forth in the Agreement.

"**Agreement**" means the agreement between Customer and Memcyco for the provision of the Memcyco SAAS Product to Customer.

"**California Privacy Statutes**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq. ("CCPA") including as amended by the California Privacy Rights Act of 2020 ("CPRA").

"**Customer Data**" has the meaning set forth in the Agreement.

"**Customer Personal Data**" means any Customer Data that is Personal Data.

"**Data Protection Laws**" means all applicable and binding privacy and data protection laws and regulations, including such laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, Canada, Israel and the United States of America, as applicable to the Processing of Personal Data under the Agreement including (without limitation) the GDPR, the UK GDPR, and the California Privacy Statutes, as applicable to the Processing of Personal Data hereunder and in effect at the time of Processor's performance hereunder.

"**EU GDPR**" means the 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).

"**GDPR**" means, solely as applicable to the particular Personal Data which is being processed, the EU GDPR, the UK GDPR or the Swiss Federal Act on Data Protection ("**Swiss FADP**").

"Memcyco" means either Memcyco Inc., a Delaware corporation having its address at 224 W 35th St., Ste 500, New York, NY 10001 or its subsidiary company which is identified in the Agreement.

"SAAS Product" has the meaning set forth in the Agreement.

"Standard Contractual Clauses" (i) the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "**EU SCCs**"), and (ii) where required by the Data Protection Law of the United Kingdom, the EU SCCs as supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018 (the "**UK Addendum**").

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" will be interpreted accordingly.

"**Security Incident**" means any unauthorized or unlawful breach of security in the SAAS Product that leads to the unauthorized disclosure of or access to Customer Personal Data.

"**Sub-processor**" means any Data Processor engaged by Memcyco or its Affiliates to assist in fulfilling its obligations with respect to providing the Memcyco SAAS Product pursuant to the Agreement or this DPA. Sub-processors may include third parties or Memcyco's Affiliates.

"**UK GDPR**" means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

The terms, "**Controller**", "**Member State**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR. The terms "**Business**", "**Business Purpose**", "**Consumer**" and "**Service Provider**" shall have the same meaning as in the California Privacy Statutes.

For the purpose of clarity, within this DPA "**Controller**" shall also mean "**Business**", and "**Processor**" shall also mean "**Service Provider**", to the extent that the California Privacy Statutes applies. In the same manner, Processor's Sub-processor shall also refer to the concept of Service Provider.

2. Scope and Applicability of this DPA

2.1 This DPA applies where and only to the extent that Memcyco Processes Customer Personal Data on behalf of Customer as Data Processor in the course of providing SAAS Product pursuant to the Agreement.

2.2 Notwithstanding expiry or termination of the Agreement, this DPA will remain in effect until, and will automatically expire upon, deletion of all Customer Personal Data by Memcyco as described in this DPA or termination of the Agreement.

3. Roles and Scope of Processing

3.1 **Role of the Parties**. As between Memcyco and Customer, Customer is either the Data Controller of Customer Personal Data, or in the case that Customer is acting on behalf of a third party Data Controller, then a Data Processor, and Memcyco shall process Customer Personal Data only as a Data Processor acting on behalf of Customer.

3.2 **Customer Processing of Personal Data**. Customer, in its use of the SAAS Products, and Customer's instructions to the Processor, shall comply with Data Protection Laws. Customer shall establish and have any and all required legal bases in order to collect, Process and transfer to Processor the Personal Data, and to authorize the Processing by Processor, and for Processor's Processing activities on Customer's behalf, including the pursuit of 'business purposes' as defined under the California Privacy Statutes. If Customer is itself a Data Processor, Customer warrants to Memcyco that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Memcyco as another Data Processor, have been authorized by the relevant Data Controller to the extent required under applicable Data Protection Laws.

3.3 **Customer Instructions**. Memcyco will process Customer Personal Data only for the purposes described in this DPA and only in accordance with Customer's lawful instructions documented in this DPA, the Agreement, and via Customer's use of the SAAS Product, and in order for Memcyco to fulfil its obligations to provide SAAS Product under the Agreement ("Customer Instructions"), unless otherwise required by applicable law. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to Memcyco in relation to the processing of Customer Personal Data. Additional processing outside the scope of these Customer Instructions (if any) will require prior written amendment to this DPA executed by Customer and Memcyco.

3.4 **Details of Data Processing.**

(a) Subject matter: The subject matter of the data processing under this DPA is the Customer Personal Data.

(b) Purpose: The purpose of the data processing under this DPA is the provision of the Memcyco SAAS Product to the Customer and the performance of Memcyco's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties in mutually executed written form.

(c) Duration: As between Memcyco and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

(d) Nature of the processing: Memcyco provides the SAAS Product, which may process Customer Personal Data upon the instruction of the Customer in accordance with the terms of this DPA, the Agreement, and Customer Instructions.

3.5 **Processing of Customer Personal Data**. Memcyco will not: (i) retain, use, or disclose Customer Personal Data or combine Customer Personal Data with Personal Data from other sources, except as necessary to maintain or provide the Memcyco SAAS Product and its obligations under the Agreement, this DPA, or as necessary to comply with the law or binding order of a governmental body; (ii) "sell" or "share" (as such terms are defined by the California Privacy Statutes) Customer Personal Data; or (iii) retain, use, or disclose Customer Personal Data other than in the context of the direct relationship with Customer in accordance with the Agreement.

4. Subprocessing

4.1 **Authorized Sub-processors**. Customer agrees that Memcyco may engage Sub-processors to provide data centers to host Customer Data and the SAAS Products application software, disaster recovery, and backup related services and to otherwise Process Personal Data on its behalf. Customer hereby consents to Memcyco's use to the Sub-processors currently utilized by Memcyco to Process Customer Personal Data. Memcyco's then-current list of the Sub-processors engaged by it and the country where each such Sub-processor is located **("Sub-Processor List")** is available at https://www.memcyco.com/home/wp-content/uploads/2022/09/Memcyco-Sub-processor-List-4-26-22.pdf

4.2 The Memcyco website contains a mechanism to subscribe to notifications of new Sub-processors for SAAS Products which can be found at https://www.memcyco.com/home/subscribe/, and if Customer subscribes, Memcyco shall provide notification of any intended addition of any new Sub-processor (whether to replace an existing Sub-processor or otherwise) to Process Personal Data in connection with the provision of the SAAS Products. If Customer does not object to such new Sub-processor by sending a notice of objection to legal@memcyco.com within 10 days thereafter, Customer shall be deemed to have consented to such new Sub-processor. If Customer reasonably objects in writing within such 10-day period to Memcyco's proposed use of such new Sub-processor, Memcyco will either (i) refrain from permitting such objected-to new Sub-processor from Processing Customer Personal Data within 30 days thereafter; or (ii) notify the Customer within 30 days thereafter that it is not able to refrain from using such objected-to new Sub-Processor without adversely impacting the applicable SAAS Products product ("**Non-Feasibility Notice**"). Upon receipt of such Non-Feasibility Notice, Customer shall have the option for a period of 30 days thereafter, to terminate upon written notice its subscription to use only those SAAS Products which cannot be provided by Memcyco without the use of the objected-to new Sub-processor. Such termination shall be without penalty or liability (other than for fees due and owing to Memcyco for any services performed prior to such termination) effective immediately upon written notice of such termination to Memcyco.

4.3 **Sub-processor Obligations**. Memcyco will: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Personal Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the

obligations of this DPA and for any breach of this DPA caused by acts or omissions of the Sub-processor to the same extent that Memcyco would be liable if such breach was committed by Memcyco.

5. Security

5.1 **Security Measures**. Memcyco shall implement and maintain appropriate technical and organizational security measures to preserve the security and confidentiality of the Customer Personal Data processed by the SAAS Product.

5.2 **Security Incident Response**. Upon confirming a Security Incident, Memcyco shall: (i) notify Customer without undue delay, and in any event such notification shall, where feasible, occur no later than 72 hours from Memcyco confirming the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) Memcyco shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Memcyco's notification of or response to a Security Incident under this Section 5.2 (Security Incident Response) will not be construed as an acknowledgment by Memcyco of any fault or liability with respect to the Security Incident.

6. Customer Responsibilities.

Customer agrees that Memcyco has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Memcyco's systems (for example, offline or on-premise storage on Customer's computers).

7. International Transfers

Memcyco hosts Customer Personal Data in the United States unless otherwise specified in the Agreement or the applicable Order Form, provided, however, that the Personal Data which pertains to a User may be transferred to and from that User's device via the Internet at any international location where such device connects to the Internet. In the event that Customer is subject to European Data Protection Law and the transfer of Customer Personal Data to Memcyco would be restricted in the absence of the Standard Contractual Clauses, the Parties agree that the Standard Contractual Clauses shall be incorporated into this DPA with Customer as the "data exporter" and Memcyco as the "data importer." The Standard Contractual Clauses are further completed as follows: the optional docking clause in Clause 7 is implemented; Clause 9(a) option 2 is implemented and the time period therein is specified as thirty (30) days; the optional redress clause in Clause 11(a) is struck; the governing law in Clause 17 is the law of the Republic of Ireland; the court in Clause 18(b) are the Courts of the Republic of Ireland; and Annex 1, 2 and 3 to the Standard Contractual Clauses are described in this DPA. Where applicable, Part 1, tables 1, 2 and 3 of the UK Addendum will be deemed to be completed like its equivalent provisions in the EU SCCs. For the purpose of Part 1, Table 4, the party that may end the UK Addendum in accordance with Section 19 of the UK Addendum is the importer.

8. Return or Deletion of Customer Data

8.1 **Deletion by Customer**. Memcyco will cooperate with Customer to enable deletion of Customer Personal Data in accordance with the procedures set forth in 9.2 below.

8.2 **Deletion on Termination.** No later than 90 days following termination or expiration of the Agreement, Customer hereby instructs Memcyco to delete all remaining Customer Personal Data stored within the data repository associated with the Customer's SAAS Product account. Memcyco shall not be required to delete Customer Personal Data to the extent (i) Memcyco is required by applicable Data Protection Laws or order of a governmental or regulatory body to retain some or all of the Customer Personal Data; and/or (ii), Customer Personal Data it has archived on back-up systems, which Customer Personal Data Memcyco shall securely isolate and protect from any further usage, except to the extent required by applicable Data Protection Laws.

9. Cooperation

9.1 The Memcyco SAAS Product includes controls that Customer and/or Memcyco may use to delete Customer Personal Data, which Customer and/or Memcyco may use to assist in connection with their respective obligations under the Data Protection Laws, including obligations relating to responding to requests from data subjects or applicable data protection authorities. In the event that any request from individuals or applicable data protection authorities is made directly to Memcyco, Memcyco shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so, and instead, after being notified by Memcyco, Customer shall respond. If Memcyco is required to respond to such a request, Memcyco will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

9.2 Customer acknowledges that Memcyco is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each Data Processor and/or Data Controller on behalf of which Memcyco is acting and, where applicable, of such Data Processor's or Data Controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, Customer will, where requested, provide such information to Memcyco.

9.3 Security Reports. Memcyco shall provide written responses on a confidential basis to reasonable requests for information made by Customer related to its Processing of Customer Personal Data related to information security and audit questionnaires necessary to confirm Memcyco's compliance with this DPA and the Data Protection Laws, provided that Customer shall not exercise this right more than once per year, and any such request shall not be made in a manner so as to interfere with Memcyco business.

9.4 Audits. Upon Customer's 14 days prior written request at reasonable intervals (no more than once every 12 months), and subject to strict confidentiality undertakings by Customer, Memcyco shall make available to Customer that is not a competitor of Memcyco (or Customer's independent, reputable, third-party auditor that is not a competitor of Memcyco and not in conflict with Memcyco, subject to their confidentiality undertakings) information necessary to demonstrate Memcyco's compliance with this DPA, and allow for audits, including inspections, conducted by them (provided, however, that such information, audits, inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Memcyco's prior written approval. Customer shall bear the cost and expense of any such audit or inspection. Upon Memcyco's first request, Customer shall return all records or documentation in Customer's possession or control provided by Memcyco in the context of the audit and/or the inspection). If and to the extent that the Standard Contractual Clauses apply, nothing in this Section 9.4 shall be deemed to vary or modify the Standard Contractual Clauses nor affect any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses.

9.5 In the event of an audit or inspections as set forth above, Customer shall ensure that it (and each of its mandated auditors) will not cause (or, if it cannot avoid, minimize) any damage, injury or disruption to Memcyco's premises, equipment, personnel and business, as applicable, while conducting such audit or inspection.

9.6 The audit rights set forth in 9.4 above, shall only apply to the extent that the Agreement does not otherwise provide Customer with audit rights that meet the relevant requirements of Data Protection Laws (including, where applicable, article 28(3)(h) of the GDPR or the UK GDPR).

9.7 In the event the Customer is required to carry out data protection impact assessments under EU Data Protection Law, Memcyco will (at Customer's request and expense), provide reasonably requested information regarding the Memcyco SAAS Product to enable the Customer to carry out such data protection impact assessments.

10. California Privacy Statutes Standard of Care; No Sale of Personal Information.

Memcyco acknowledges and confirms that it does not receive or process any Customer Personal Data as consideration for any services or other items that Memcyco provides to Customer under the Agreement. Memcyco shall not: (i) retain, use, or disclose Customer Personal Data or combine Customer Personal Data with Personal Data from other sources, except as necessary to maintain or provide the Memcyco Hosted Service and its obligations under the Agreement, this DPA, or as necessary to comply with the law or binding order of a governmental body; (ii) "sell" or "share" (as such terms are defined in the California Privacy Statutes) any Customer Personal Data Processed hereunder without Customer's prior written consent; or (iii) retain, use, or disclose Customer Personal Data other than in the context of the direct relationship with Customer in accordance with the Agreement. Memcyco shall comply with the California Privacy Statures as applicable to it and notify Customer if it determines that it can no longer meet its obligations under the California Privacy Statutes.

11. Relationship with the Agreement

11.1 Precedence. The parties agree that DPA shall replace any existing DPA the parties may have previously entered into in connection with the Memcyco SAAS Product. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with its subject matter.

11.2 Liability. The liability of each party and each party's Affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement.

11.3 Applicable Law. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

11.4 Termination. This DPA will continue for so long as Memcyco is hosting, storing and/or processing Customer Personal Data in connection with the Agreement.

[End of main body of this DPA. Annexes follow]

ANNEX 1

This Annex forms part of the Standard Contractual Clauses.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Annex.

A. LIST OF PARTIES

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is the party identified as the "Customer" in the Agreement and/or this DPA between Memcyco Ltd. and such Customer.

Data Exporter's address and contact information are set forth in the Agreement and/or this DPA.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Memcyco Ltd., an Israeli corporation having its address at 21 Bar Kochva Street, 10th Floor, Bnei Brak 5126001, Israel

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

All Individuals ("Users") who (i) access the Data Exporter's website(s) which are enabled with Data Importer's SAAS Product(s), and/or (ii) receive electronic communications from Data Exporter on a communications platform which is enabled with Data Importer's SAAS Product(s).

Categories of personal data transferred.

PoSA™ for Websites.

Data Importer (Memcyco) provides its customers with a software-as-service (SAAS) that enables the customer website to show a watermark with a unique code for each user who visits that website so that user can be assured that he or she is viewing the authentic website (and not a counterfeit website).

To achieve this functionality, the following data is stored and processed by Data Importer:

1. The user ID that the user enters to log-in to the customer website (or an automatically assigned user ID if the customer website does not require log in or registration).
2. Information which identifies the computer that is being used to access the customer website (e.g., IP address, hardware, operating system, browser type)
3. The location range reflected by the IP address of the computer that is being used to access the customer website.
4. The time when such computer is being used to access the customer website.

It is important to note that Data Importer does not store or process the unique user code.

PoSA™ for Email and Text Messaging.

Data Importer (Memcyco) provides its customers with a SAAS plug-in to their mail merging software platform (e.g. Mailchimp) which populates each email or text message in a batch (prior to sending) with a watermark with a unique code for each recipient so the recipient can be

assured that the email or text message received is from the legitimate source (and not an impersonating source). Memcyco PoSA™ for Email and Text Messaging does not send out emails or text messages to the customer's recipients.

To achieve this functionality, the following data is stored and processed by Data Importer:

1. The user ID that the recipient has previously entered in the registration framework that the customer uses to register that recipient for this PoSA™ watermark verification system.
2. The watermark and recipient code that is inserted into the message for each recipient.

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.

None

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

Continuous

Nature of the processing

The SAAS Product(s) that the Data Importer provides consists a suite of standardized software as a service (SAAS) applications which are used: (i) to provide Users who access the Data Exporter's website(s) with verification and assurance that they are accessing the Data Exporter's authentic website (and not a fraudulent imposter website) ("Proof of Source Authenticity"), (ii) to provide Proof of Source Authenticity to recipients of certain electronic communications originating from the Data Exporter using communication platforms that are licensed , and (ii) provide security related alerts to Data Exporter and/or such Users. The range of functions available for processing the data are limited to the features and functionality of the standard SAAS application.

Purpose(s) of the data transfer and further processing

Cybersecurity and Proof of Source Authenticity.

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

Term of the services contract and for an amount of time thereafter that is reasonable and appropriate to fulfill the processor's obligations under the contract.

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

Data centers in the cloud and/or co-location data centers to host the application and process data. Disaster recovery and data backup services. Third party application functionality.

C. COMPETENT SUPERVISORY AUTHORITY

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

To be determined in accordance with Clause 13 (Supervision) of the Standard Contractual Clauses depending on the location of Data Exporter.

ANNEX 2

This Annex forms part of the Standard Contractual Clauses.

Data importer shall implement a comprehensive and current Personal Data protection and security program to ensure reasonable and appropriate protection of the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, particularly where the processing involves the transmission of the Personal Data over a network, and against all other unlawful forms of processing. Data importer hereby undertakes to use commercially reasonable efforts to:

1. prevent any unauthorised person from accessing the facilities used for data processing (monitoring of entry to facilities);
2. prevent data media from being read, copied, amended or moved by any unauthorised persons (monitoring of media);
3. prevent the unauthorised introduction of any data into the information system, as well as any unauthorized knowledge, amendment or deletion of the recorded data (monitoring of memory);
4. prevent data processing systems from being used by unauthorised persons using data transmission facilities (monitoring of usage);
5. ensure that authorised persons, when using an automated data processing system, may access only those data that are within their competence (monitoring of access);
6. ensure the checking and recording of the identity of third parties to whom the data can be transmitted by transmission facilities (monitoring of transmission);
7. ensure that the identity of all persons who have or have had access to the information system and the data introduced into the system can be checked and recorded ex post facto, at any time and by relevant persons (monitoring of introduction);
8. prevent data from being read, copied, amended or deleted in an unauthorised manner when data are disclosed and data media transported (monitoring of transport); and
9. safeguard data by creating backup copies (monitoring of availability).

It is acknowledged that the foregoing technical and organisational measures are subject to technical progress, organisational changes, and other developments, and the Data Importer may implement adequate alternative measures if these measures do not derogate from the level of protection contractually agreed upon.

ANNEX 3

This Annex forms part of the Standard Contractual Clauses.

The controller has authorised the use of the sub-processors listed at: https://www.memcyco.com/home/wp-content/uploads/2022/09/Memcyco-Sub-processor-List-4-26-22.pdf