Information Commissioner's Office

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

UK 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 set forth in the Agreement and Data Processing Addendum between the parties. Trading name (if different):	Full legal name: **"Memcyco"** which means either Memcyco Inc., a Delaware corporation having or its subsidiary company which is identified in the Agreement and/or the Data Processing Agreement with the Data Exporter. Trading name (if different):

	Main address (if a company registered address): As set forth in the Agreement and Data Processing Addendum between the parties. Official registration number (if any) (company number or similar identifier):	Main address (if a company registered address): 224 W 35th St., Ste 500, New York, NY 10001 or such other address which is identified in the Agreement and/or the Data Processing Agreement with the Data Exporter Official registration number (if any) (company number or similar identifier):

Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional):Scott Lenga Job Title: General Counsel Contact details including email:Scott@memcyco.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	x The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: April 2022 Reference (if any): add url for EU standard clauses 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		Included	Decline to include	General Authorisation	Term of Service Contract and reasonable period afterward to perform obligations after	Yes

					termination of contract	
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 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 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" which 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 and/or the Data Processing Agreement with the Data Exporter.

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). Data Importer 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 III – LIST OF SUB-PROCESSORS

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

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: X Importer X Exporter neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate	The standard of protection over the personal data and

Safeguards	of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum 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.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one

meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of

Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory 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.	**Clauses**