CUSTOMER DATA PROCESSING ADDENDUM

This Customer Data Processing Addendum ("**DPA**") forms part of the Agreement between Moosend LTD, a wholly owned subsidiary under Sitecore Corporation A/S ("**Moosend**") and Customer ("**Customer**"), together referred to as the Parties ("**Parties**") and applies where Moosend will process Customer Data (including Personal Data, as defined below) when providing Services under the Agreement. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

This DPA becomes binding on the Parties on the Effective Date of the Agreement and shall remain in effect for the duration of the Agreement, including any retrieval or extended access period necessary for data return or deletion.

1. DEFINITIONS

"Agreement" means the written or electronic agreement between Customer and Moosend for the provision of the Services to Customer.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code §1798.100 et seq., and its implementing regulations.

"Customer Data" is defined in the Agreement.

"Data Subject" or **"Data Subjects"** means an identified or identifiable natural person who can be identified directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data or an online identifier or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. A legal person may qualify as a Data Subject under Data Protection Laws and Regulations of specific jurisdictions. This includes, to the extent applicable, any analogous variations of such terminology, such as "**Consumer**" as may be relevant under US state laws.

"Data Exporter" means the Party identified as **"Customer"** in the Agreement, a customer of the Services of the Data Importer.

"Data Importer" is **Moosend**, a provider of experience management software, and its Affiliates.

"Data Protection Laws and Regulations" means all laws and regulations, including the laws and regulations of the European Union, the European Economic Area (hereinafter, the "**EEA**") and their member states, Switzerland, the United Kingdom, Australia, Canada, and the United States and its states, applicable to the Processing of Personal Data under the Agreement as amended from time to time.

"Data Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller, including as applicable any "Service Provider" as defined herein.

"International Data Transfer Addendum" (hereinafter, "IDTA") means the UK Addendum to the Standard Contractual Clauses, which is considered to provide appropriate safeguards to the transfer of Personal Data from the United Kingdom to third countries in accordance with the Data Protection Laws and Regulations of the UK.

"Personal Data" means any Customer Data relating to an identified or an identifiable natural person or as otherwise defined under Data Protection Laws and Regulations. For the sake of clarity, where applicable, this includes **"Personal Information"** or analogous variations of such terminology within the meaning of applicable US state laws, to the extent that these may be applicable.

"Processing" or "Process" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Security Incident" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data transmitted, stored, or otherwise Processed. Security Incident does not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"Service Provider" has the meaning set forth in Section 1798.140(v) of the CCPA.

"Services" as used in this DPA means the "SaaS Products" and/or "Hosted Services" as defined in the Agreement.

"Subprocessor" means any Data Processor or Service Provider (where applicable) engaged by Moosend or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Subprocessors may include third parties detailed on Annex B or Affiliates of Moosend.

"Standard Contractual Clauses" means 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, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

2. SCOPE OF THIS DPA

This DPA applies where Moosend Processes Customer Data, including Personal Data, on behalf of Customer in the course of providing Services to the Customer pursuant to the Agreement.

3. ROLES AND SCOPE OF PROCESSING

3.1 **Role of the Parties**. As between Moosend and Customer, Customer is the Data Controller of Customer Data and Moosend shall Process Customer Data only as a Data Processor acting on behalf of Customer. For the avoidance of doubt, this DPA shall not apply to any instances where Moosend is acting as a Data Controller (as defined under applicable Data Protection Laws and Regulations).

3.2 **Customer's obligations.** Customer shall have the sole and exclusive authority to determine the purposes and means of Processing Customer Data transferred or otherwise disclosed to Moosend. As between the Parties, the Customer shall have the sole responsibility for the accuracy, quality and legality of Personal Data as required by applicable Data Protection Laws and Regulations and the means by which the Customer acquired Personal Data, including the provision of proper notice and obtaining consents where appropriate for Processing by Moosend.

3.3 **Moosend Processing of Customer Data.**

(a) **Treated as confidential:** Moosend will maintain confidentiality of Customer Data.

(b) **Processing to follow Customer instructions:** Moosend shall Process Customer Data only for the purpose of providing the Services and in accordance with Customer's documented lawful instructions, as set forth in the Agreement and this DPA. The categories of Personal Data, categories of Data Subjects and the purposes of the Processing are as set out in **Annex C** for the sake of clarity this expressly excludes Restricted Data as defined in the Agreement). The Parties agree that the Customer's complete and final instructions with regard to the nature and purposes of the Processing are set out in this DPA unless (or except as) required under applicable laws. Processing outside the scope of these instructions (if any) will require prior written agreement between Customer and Moosend with additional instructions for Processing.

(c) **Moosend does not sell Personal Data:** Moosend shall not:
(i) sell or rent Customer Personal Data;
(ii) retain, use, or disclose the Personal Data for any "business purpose" (as defined in the CCPA §1798.140(d)), or any "commercial purpose" (as defined in the CCPA §1798.140(f)) other than for the specific purpose of performing the Services under the Agreement, and as instructed by Customer, pursuant to Section 3.3 (b) above, or
(iii) retain, use, or disclose Customer Data outside of the direct business relationship between Moosend and Customer except to the extent as may be required by applicable laws and regulations.

(d) **Security Measures and adequate safeguards:** Moosend represents that it has implemented adequate technical and organizational measures necessary to secure Customer Data, including, as appropriate, the Security Measures (defined in Section 5 below) referenced in Data Protection Laws and Regulations and more fully described at **Annex A** to this DPA.

3.4 **Details of Data Processing**

(a) **Subject matter:** The subject matter of the Processing under this DPA is Customer Data, as detailed in **Annex C**.

(b) **Duration:** As between Moosend and Customer, the duration of the Processing under this DPA is the term of the Agreement or as otherwise agreed upon by the Parties.

(c) **Purpose:** The purpose of the Processing under this DPA is the provision of the Services to the Customer and the performance of Moosend's obligations under the Agreement and this DPA (or as otherwise agreed by the Parties) and more fully described at **Annex C** to this DPA.

4. SUBPROCESSING

4.1 **Authorized Subprocessors.** Customer agrees that in order to provide the Services, Moosend may engage Subprocessors to Process Customer Data. A list of Moosend's current authorized Subprocessors is found in **Annex B**. Moosend maintains a current list of its Subprocessors on its website here and will email Customers and post notifications of any new or replacement Subprocessors, prior to the use or replacement of Subprocessors.

4.2 **Subprocessor Obligations.** Where Moosend authorizes any Subprocessor as described in Section 4.1:

(a) **Restricted to a need-to-know:** Moosend will restrict the Subprocessors access to Customer Data only to what is necessary to assist Moosend in providing or maintaining the Services, and will prohibit the Subprocessor from Processing Customer Data for any other purpose;

(b) **Moosend due diligence:** Before any Subprocessor first Processes Customer Data, Moosend shall carry out adequate due diligence to ensure that the Subprocessor is capable of providing the same level of protection for Customer Data required by the Agreement and this DPA;

(c) **Entry into written agreements:** Moosend will enter into a written agreement with the Subprocessor imposing data protection terms that places the equivalent data protection obligations as those set out in this DPA to the extent applicable to the nature of the services provided by such Subprocessor, in particular providing appropriate technical and organisational measures that the Processing will protect the Customer Data to the standard required by Data Protection Laws and Regulations;

(d) **Liability for Subprocessors:** Moosend will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor that cause Moosend to breach any of its obligations under this DPA; and

(e) **Objection Right for new Subprocessors:** If Customer has a reasonable basis relating to privacy or data security to object to Moosend's use of a new or replacement Subprocessor, Customer shall notify Moosend promptly in writing within 30 business days after such notice being made by Moosend on its website of a new or replacement Subprocessor. In the event Customer objects to any new Subprocessor(s) on such grounds, Moosend will use reasonable efforts to work in good faith with Customer to find an acceptable, commercially reasonable, alternate solution. If the Parties are not able to agree to an alternate solution within a reasonable time (no more than 90 days from Moosend's receipt of notice of Customer's objection), Moosend will either not appoint or replace the Subprocessor or, if this is not possible, Customer may suspend or terminate the applicable Order for Services in respect only to the specific Services which cannot be provided by Moosend without the use of the objected-to new Subprocessor, by providing written notice to Moosend and without prejudice to any fees incurred by Customer prior to suspension or termination.

5. SECURITY MEASURES AND SECURITY INCIDENT RESPONSE

5.1 **Security Measures.** Moosend has implemented and will maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of Customer Data ("**Security Measures**"). The Security Measures applicable to the Services are set forth in **Annex A** as updated or replaced from time to time in accordance with Section 5.2. Customer is responsible for reviewing the information made available by Moosend relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws and Regulations, taking into account the nature, scope, context and purposes of Processing, as well as, the risks associated with the contracted Processing.

5.2 **Updates to Security Measures.** Moosend has implemented a procedure for the regular testing, inspection, assessment, and evaluation of the effectiveness of Moosend's Security Measures. Accordingly, Customer acknowledges that the Security Measures are subject to technical progress and development and that Moosend may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer. Such updates to the Security Measures will be made available to Customer upon its reasonable request.

5.3 **Personnel.** Moosend shall take reasonable steps to ensure the reliability of any Personnel who may have access to Customer Data, ensuring that access is strictly limited on a least-privilege basis to those individuals who need to know or need to have access to Customer Data as is

necessary for the provision of the Services under the Agreement. Further, Moosend shall ensure that Personnel with access to Customer Data are under an appropriate obligation of confidentiality and that such Personnel have received appropriate data protection and security training pertaining to the responsibilities of their role.

5.4 **Customer Responsibilities.** Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

5.5 **Sufficient Evidence**. Upon the reasonable request of Customer, Moosend shall provide Customer with sufficient information to enable Customer to demonstrate that the necessary technical and organizational security measures (as further detailed in **Annex A**) have been implemented.

5.6 **Security Incident Response.**

(a) **Notification:** Upon becoming aware of a Security Incident, Moosend will notify Customer without undue delay (and no later than 48 hours after becoming aware of the Security Incident) and will provide information relating to the Security Incident as it becomes known or as is reasonably requested by Customer including:

(i) details of the Customer Data compromised, including whether the Customer Data had been encrypted, hashed or otherwise rendered incomprehensible, inaccessible or unintelligible for unauthorized persons,
(ii) information on the Data Subjects affected, such as categories and the number of Data Subjects affected,
(iii) the categories and number of information data records affected,
(iv) description of the nature of the Security Incident,
(v) identity and contact details of Moosend's Privacy contact,
(vi) when the Security Incident took place (date or time period) and suspected cause,
(vii) the likely consequences of the Security Incident, and
(viii) any recommendations to minimize harm.

(b) **Assistance:** Moosend will also take reasonable steps to mitigate and, where possible, to remedy the effects of, any Security Incident. Moosend shall provide reasonable assistance to Customer, in the event Customer is required under Data Protection Laws and Regulations to notify a data protection authority or any Data Subjects of a Security Incident.

6. REPORTS AND AUDITS

6.1 Upon Customer's request, Moosend will make available a statement from its Security Team containing all information necessary to demonstrate compliance with this DPA (a "**Moosend Report**") and any documentation pursuant to Section 10.

6.2 No more than once per year, Customer may conduct reviews of Moosend's documents and systems, by way of desk-based questionnaires and phone conferences with Moosend Personnel.

6.3 Notwithstanding the foregoing, Customer will have the right, at its expense, to conduct an onsite audit, only in the event that:

(a) Customer reasonably believes that Moosend is out of compliance with this DPA, or

(b) Customer is subject to a regulatory audit, government investigation, court order or otherwise mandatory audit under applicable Data Protection Laws and Regulations that includes the scope of this DPA. Any on-site audit will be conducted during normal business hours, at a date and time as mutually agreed between the Parties, and only if such an audit at Moosend's premises is necessary to prove facts or otherwise demonstrate applicable compliance that Moosend cannot otherwise evidence through a Moosend Report, desk-based questionnaires, phone conferences, third-party certification programs or third-party audit reports. Customer agrees that with respect to any Moosend Confidential Information received in connection with such audit, Customer will be subject to the same confidentiality obligations as set forth in the Agreement.

7. INTERNATIONAL TRANSFERS

7.1 **Data Centre Locations.** Customer understands that Customer Data within the Services will be Processed, transferred to and stored wherever Customer chooses to have Customer Data hosted, and Moosend shall store Customer Data only in the Customer selected data

centre (and as detailed on any applicable Order Form) locations unless notified otherwise. Moosend further confirms that Customer Data will not be transferred from the data centre location chosen by Customer without Customer's prior consent.

7.2 **Data Transfers.** If applicable, Moosend will at all times ensure that any Customer Data which is transferred is done so in compliance with adequate transfer mechanisms. Where applicable, Moosend has put in place supplemental technical and organisational measures to ensure that any Customer Data being transferred using our services is afforded an adequate level of protection in the destination country in accordance with the requirements of Data Protection Laws and Regulations. Details of these supplemental measures are located in Section 9, below, and at Annex A of this DPA.

7.3 **Data Transfer Mechanisms (to the extent applicable).** The Parties agree that the Standard Contractual Clauses in **Annex D** to this DPA shall be the adequate transfer mechanism pursuant to Section 7.2 above and apply to Personal Data that is transferred from the EEA and/or Switzerland to outside the EEA and Switzerland, either directly or via onward transfer, to any country or recipient not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the Data Protection Laws and Regulations).

7.4 **Swiss Addendum to the EU Commission Standard Contractual Clauses (to the extent applicable).** For transfers of Personal Data in compliance with the Federal Act on Data Protection 1992 ("FADP"), the parties agree that the Standard Contractual Clauses supplemented by the Swiss Addendum to the EU Commission Standard Contractual Clauses are the appropriate transfer mechanism.

7.5 **Restricted Transfers Under UK GDPR (to the extent applicable).** For transfers of Personal Data in compliance with section 119(A)and article 46 of the Data Protection Act 2018, the parties agree that the Standard Contractual Clauses supplemented by the UK International Data Transfer Addendum (IDTA) are the appropriate transfer mechanism.

8. RETURN OR DELETION OF DATA

Moosend's obligations regarding the return or deletion of Customer Data are as set forth in the Agreement. Upon termination of the Agreement, Moosend may retain Customer Data in a manner that restricts the Processing solely to the extent that it may be necessary to comply with applicable law or regulation. This should not apply to Customer Data that has been archived on back-up systems, which Customer Data Moosend shall securely isolate and protect from any further Processing, except to the extent required by applicable laws and regulations.

9. PRIVACY RIGHTS

9.1 To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Moosend shall provide reasonable and timely cooperation to assist Customer to respond to any requests from individuals, applicable supervisory authorities or relevant regulators relating to the Processing of Personal Data under the Agreement. In the event any such request is made directly to Moosend, a Moosend Affiliate or any Subprocessor, Moosend shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Moosend is required to respond to such a request, Moosend will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so, for example to preserve the confidentiality of an investigation by law enforcement authorities.

9.2 If a law enforcement agency sends Moosend a demand for Customer Data (for example, through a subpoena or court order), Moosend will attempt to redirect the law enforcement agency to request such Customer Data directly from Customer. As part of this effort, Moosend may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Moosend will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Moosend is legally prohibited from doing so.

9.3 Moosend shall, upon Customer request and at Customer's expense, provide reasonable assistance to Customer needed to fulfil any Customer obligation under the applicable Data Protection Laws and Regulations to perform any data protection impact assessments. Moosend shall, upon Customer request, provide reasonable assistance to Customer in any prior consultations with supervising authorities or other competent data privacy authorities, which Customer reasonably considers to be required of Customer under Data Protection Laws and Regulations.

10. PRIVACY AND DATA PROTECTION

Moosend maintains a privacy program that includes dedicated resourcing, audit, and review processes designed to implement appropriate privacy controls and procedures, including but not limited to:

(a) **Designated individual**: The designation of an employee or employees to coordinate, provide oversight and be responsible for the privacy program;

(b) **Data Protection Officer**: Moosend retains a Data Protection Officer (DPO) who can be contacted via email at privacy@sitcore.com.

(c) **Privacy risk assessments**: The identification of reasonably foreseeable, material risks, both internal and external, that could result in unauthorized collection, use, or disclosure of Personal Data, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in:

i. employee training and management,
ii. product design, development, and research and,
iii. adequacy of security controls.

(d) **Testing of Effectiveness**: The design and implementation of reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, will be subject to and regular testing and monitoring of the effectiveness of those privacy controls and procedures; and

(e) **Reviews:** Moosend will evaluate and adjust the privacy program to address any known change of circumstances that may have a material impact on the effectiveness of the privacy program.

11. COMPLIANCE WITH THIS DPA

11.1 Moosend shall maintain appropriate documentation necessary to demonstrate Moosend's compliance with this DPA (including certifications, independent audit report summaries and policy tables of content) and make such documentation, subject to redaction of Confidential Information not relevant to the requirements of this DPA, available to Customer upon its reasonable request.

11.2 Customer may request on annual basis, that Moosend shall provide to Customer such copies of Moosend's agreements with Subprocessors referred to in Section 4 (which may be redacted to remove Confidential Information not relevant to the requirements of this DPA).

11.3 Each Party shall appoint an individual within its organisation authorised to respond from time to time to enquiries regarding the Personal Data and each Party shall deal with such enquiries promptly.

11.4 Moosend shall make reasonable efforts to notify Customer if it becomes aware of any possible violation of, or inability to comply with, this DPA, Data Protection Laws and Regulations or Customer instructions.

12. CONTACT

12.1 Customer may contact Moosend's Security Team in relation to any Security Incident, notification or security question by emailing **security@sitecore.com**.

12.2 All other queries relating to this DPA should be directed to **privacy@sitecore.com**.

13. GENERAL

13.1 For the avoidance of doubt, any claim or remedies either party may have against the other party arising under or in connection with this DPA, will be subject to the limitation of liability provisions set forth in the Agreement.

13.2 Any claims against Moosend or its Affiliates under this DPA shall be brought solely against the entity that is a Party to the Agreement. In no event shall any Party limit its liability with respect to any individuals' data protection rights under this DPA or otherwise.

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

13.4 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.

13.5 Upon termination of the Agreement, and the cessation of any Services to the Customer, the respective rights and obligations of the Parties shall survive until Customer Data is deleted.

IN WITNESS WHEREOF, the Parties have caused this DPA to be executed by their authorized representative effective as at the date last executed below.

Moosend LTD	**Customer**
By: _____	By: _____
Name: Panos Melissaropoulos	Name:
Title: Vice President	Title:
Date: _____	Date: _____

ANNEX A
TECHNICAL AND ORGANISATIONAL MEASURES

The term "**implemented**" refers to the existence of technical or procedural controls, designed to safeguard Customer Data and which are used to operate the Processing Environments.

Technical and Organizational Security Measure	Evidence
Measures of pseudonymisation and encryption of Customer Data	Moosend has implemented the following measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking (e.g., database security, transmission security): (a) **Encryption:** Encryption mechanisms are used for data in storage+ and in transmission (e.g., TLS). Encryption is managed in accordance with industry best practices, including: (i) Maintaining secure encryption key management processes that require the encryption/decryption key to be: (A) Managed independently of the native operating system access control system; (B) Stored securely and adequately protected with strong access controls; (C) Secured during transmission or distribution; (D) Changed once keys have expired; (E) Retired or replaced if the integrity of the key has been weakened or compromised (including replacement of the key if an employee with knowledge of the key leaves the organization); and (F) Whole disk encryption on all portable Moosend systems containing Customer Data.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services	Moosend has implemented and will maintain a comprehensive written information security program, designed to comply with applicable law, industry standards and best practices. This program includes the following controls as part of its security governance: (a) **Objectives of the security program:** The security program will include appropriate administrative, logical, technical, physical, and organizational safeguards reasonably designed to: (i) Ensure the security, confidentiality, integrity, availability and resilience of Customer Data; (ii) To protect against any threats or hazards to the security or integrity of Customer Data in Moosend's possession; and (iii) To prevent unauthorized or accidental access, destruction, loss, deletion, disclosure, alteration, or use of Customer Data. (b) **Certifications:** Moosend's parent company, Sitecore, maintains the current certifications detailed on the Privacy and Security page, requiring annual audit by an independent third-party. (c) **Governance team:** Moosend's Security Team, led by Sitecore's Data Protection and Security Counsel (composed of members of Sitecore's Executive Team), includes members from data protection, product security, legal, IT security, global workplace, security engineering and security operations. (d) **Processes:** Moosend maintains several policies, including an Information Security Policy, designed to maintain consistent controls while governing Moosend's security program. (e) **Risk assessment:** Moosend maintains a risk assessment program to identify information security risks relating to its business, including ET systems, networks, product and business practices. (f) **Policies:** Moosend shall upgrade and in no way degrade controls from that stated on the Privacy and Security Page. (g) **Reviews:** This security program is reviewed at least annually or upon any material change in the provision of the Services to determine whether additional controls are to be implemented to address any new risks that such updates or business changes might introduce. (h) **Threat Intelligence:** Moosend monitors threats and risks pertaining to the business to help identify threats that may require preventative action.
Measures for ensuring the ability to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident	Moosend has implemented the following measures to assure data security (physical/logical): (a) **Backup:** Secure backup procedures are maintained in its Processing Environments, including: (i) Storing backup media in an off-site, backup or alternate facility, with such facility being reviewed at least annually; (ii) Physically securing all backup media; and (iii) Maintaining inventory logs and inventories of backup media.

	(b) **Availability:** Processes are in place to monitor availability of systems in Moosend's Processing Environments. (c) **Capacity Management:** Rules are in place to manage capacity in Moosend's Processing Environments. (d) **Business Continuity and Disaster Recovery:** Moosend has established Business Continuity Planning (BCP) and Disaster Recovery (DR) plans to ensure the service remains operational during disruptions. These plans include securely maintaining and testing alternate sites and infrastructure. Moosend conducts annual BCP and DR tests to ensure our plans are current and effective.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Moosend utilizes Microsoft Azure and Amazon Webs Services (AWS) to provide our cloud infrastructure. Moosend maintains contractual provisions with these vendors to provide the Moosend Services in accordance with this Moosend Customer DPA. These vendors ensure that robust physical security measures are deployed, namely: (a) **AWS Physical Security Measures**: AWS ensures the security of its data centers with a robust set of physical security controls, which include: (i) **Strict Access Control**: Access to data centers is tightly regulated using multi-factor authentication, including biometric scanning, badges, and regular audits. Only authorized personnel are allowed access. (ii) **24/7 Surveillance** AWS data centers are monitored with extensive video surveillance and intrusion detection systems, ensuring that any unauthorized access attempts are promptly identified. (iii) **Environmental Controls**: These facilities are equipped with automated systems for fire detection and suppression, climate control, and power backup, ensuring the safety of hardware. (iv) **Redundant Power and Networking**: AWS data centers have multiple power and network providers to ensure continuity in the event of failures. For more details, AWS outlines its physical security on its compliance page: [AWS Physical Security](https://aws.amazon.com/compliance/data-center/controls/) (b) **Microsoft Azure Physical Security Measures:** Microsoft Azure's physical security at its data centers includes: (i) **Physical Barriers** Azure data centers are protected with fencing, vehicle barriers, and security guards to prevent unauthorized physical access. (ii) **Multi-Factor Access Control**: Similar to AWS, Azure requires multiple layers of access control such as biometric scans and keycards. Access is granted only to authorized personnel, tracked through logs. (iii) **Surveillance and Monitoring**: Continuous video surveillance and physical audits are performed to detect and prevent unauthorized activities. Moosend has established the following measures to implement and operate a secure network, i.e., operating system that has controls to protect the applications and data that it stores and processes: (a) **Malware and anti-virus:** This includes a hardened operating system with firewalls and anti-virus systems as appropriate to protect Moosend's network, comprising the following controls: (i) Changing all manufacturer-supplied defaults before implementing into Processing Environments hosting, including but not limited to custom test accounts, default system or default user accounts, unnecessary functionality, and default encryption/decryption keys; (ii) Securing Moosend systems according to industry accepted system hardening standards and keep current as change occurs in the Processing Environment; (iii) Running antivirus software and other antivirus and anti-malware controls on all systems operating in the Processing Environment; (iv) Antivirus software is kept current and active, without the ability to be turned off or disabled. (v) Antivirus agents is configured to receive definition file updates at least once a day. (vi) Any system that is decommissioned (or repurposed for another Moosend customer) must be sanitized in accordance with NIST 800-88, Guidelines for Media Sanitation; (vii) Servers in the Processing Environment must have technical controls to prohibit email usage and/or Internet browsing by end users; and (viii) Databases part of the Processing Environment must have segmentation controls which prohibit direct access to or from the Internet. (ix) All mobile devices (including laptops, tablets, or phones) used to access or store Customer Data must be secured with appropriate encryption. (b) **Vulnerability Management:** This includes a vulnerability management program, to detect and mitigate vulnerabilities in the platform in its Processing Environments comprising the following: (i) Moosend will apply all relevant security patches to Processing Environments in accordance with criticality: (ii) Critical or High rated patches will be applied within 30 days of release date; (iii) Medium rated patches must be applied within 90 days of release date;

	(iv) Moosend uses a vulnerability scanning tool that complies with industry standards to validate security of Processing Environments; (v) External scanning must occur at least quarterly; (vi) Internal scanning must occur at least monthly; (vii) Critical or High rated vulnerabilities will be addressed within 30 days of discovery; and (viii) Medium rated vulnerabilities must be addressed within 90 days of discovery. (c) **Security Monitoring:** A SIEM tool is used for 24x7 security monitoring.
Measures for user identification and authorisation	Moosend has implemented the following technical (ID/password security) and organizational (user master data) measures for user identity management and authentication: (a) **Authentication and Authorization:** Controls are in place to secure authentication and authorize permission for access to Processing Environments, including utilizing: (i) A federated identity management solution is used for access to its Processing Environments, and where applicable, includes multifactor authentication mechanisms, including: (A) To secure delivery of data used to authenticate users during the user registration process. Emailed passwords must technically enforce one-time use. (B) Upon execution of a password reset, invalidate any previous sessions and redirect the user to the login page. (C) Unique IDs for access by Moosend Employees to Processing Environments. Shared or "group" credentials for access to Processing Environments are prohibited. *# (D) Define and adhere to identity verification and appropriate workflow for access requests to Moosend systems by its Personnel. (b) **Access controls:** Using centralized directory services, role-based access controls, which are reviewed quarterly, are used in Processing Environments to: (i) Immediately revoke access to Processing Environments of any Moosend Personnel that is terminated or changes roles; (ii) Audit access lists to Processing Environments at least quarterly to ensure proper off boarding; (iii) Grant only the minimum access privileges required based upon the requestor's job responsibilities; (iv) Processing Environments must always deny user access by default and then build permission sets as needed; and (v) Logging requests for access to Moosend systems and maintaining them in accordance with Moosend's retention policies and must include relevant log information such as user ID, approving manager's name (where appropriate), timestamp, and description (where appropriate). (c) **Passwords:** Password security standards are used in its Processing Environments including: (i) Specified password complexity rules and length; (ii) Minimum password age and expirations; (iii) Lockout policies for access attempts; (iv) Password history requirements to prevent new passwords that are identical to prior passwords for the same account; (v) Securely storing all account passwords used for oversight and management of Moosend systems in an encrypted password vault; and (vi) Auditing all password retrievals from the aforementioned password vault and maintain relevant logs.
Measures for the protection of data during transmission	Moosend has implemented procedures (Encryption Policy) to protect data during transmission to/from its Processing Environments. Data in motion is encrypted using Industry standard SSH/SCP or TLS 1.2 and above.
Measures for the protection of data during storage	Moosend has implemented procedures (Encryption Policy) to protect data stored in its Processing Environments. All data captured is encrypted using 256-bit AES (Advanced Encryption Standard) encryption, one of the strongest block cyphers available.
Measures for ensuring physical security of locations at which Personal Data are processed	Moosend utilizes Amazon Webs Services (AWS) and Microsoft Azure to provide our cloud infrastructure. Moosend maintains contractual provisions with these vendors to provide the Moosend Services in accordance with this Moosend Customer DPA. These vendors ensure that robust physical security measures are deployed, namely: (a) **AWS Physical Security Measures**: AWS ensures the security of its data centers with a robust set of physical security controls, which include: (i) **Strict Access Control**: Access to data centers is tightly regulated using multi-factor authentication, including biometric scanning, badges, and regular audits. Only authorized personnel are allowed access. (ii) **24/7 Surveillance** AWS data centers are monitored with extensive video surveillance and intrusion detection systems, ensuring that any unauthorized access attempts are promptly identified.

	(iii) **Environmental Controls**: These facilities are equipped with automated systems for fire detection and suppression, climate control, and power backup, ensuring the safety of hardware. (iv) **Redundant Power and Networking**: AWS data centers have multiple power and network providers to ensure continuity in the event of failures. For more details, AWS outlines its physical security on its compliance page: [AWS Physical Security](https://aws.amazon.com/compliance/data-center/controls/) (b) **Microsoft Azure Physical Security Measures:** Microsoft Azure's physical security at its data centers includes: (i) **Physical Barriers** Azure data centers are protected with fencing, vehicle barriers, and security guards to prevent unauthorized physical access. (ii) **Multi-Factor Access Control:** Similar to AWS, Azure requires multiple layers of access control such as biometric scans and keycards. Access is granted only to authorized personnel, tracked through logs. **(iii) Surveillance and Monitoring:** Continuous video surveillance and physical audits are performed to detect and prevent unauthorized activities**.** **(iv) Environmental Safeguards:** Data centers have advanced fire prevention systems, cooling mechanisms, and power redundancy to protect against environmental risks. **For comprehensive information, refer to the Microsoft Azure Trust Center:** **[Microsoft Azure Physical Security](https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security)** Moosend has implemented the following technical and organizational measures to control access to premises and facilities, particularly to check authorization: (a) **Physical security controls:** Physical security controls will be documented and maintained over all facilities where Customer Data is Processed to restrict access to servers, network ports, wireless access points, routers, firewalls, or any physical computing equipment involved in the provision of Services, including at a minimum, appropriate alarm systems, access controls, visitor access procedures, security guard force, fire suppression and CCTV video surveillance. (b) **Badge card access systems:** These are used to protect Processing Environments hosting Customer Data by limiting access to Moosend premises to those with a badge card and valid entry of numerical code on control panels. (c) **Visitor Management:** Protocols designed to provide supervision of all visitors to Moosend premises, both at reception areas and building entry points, are in place. This includes completion of NDA where appropriate, maintenance of visitor logs (with date, time duration, visitor name, company, and onsite personnel escort identification). (d) **CCTV:** Egress points and server rooms are subject to 24/7/365 video surveillance. (e) **Physical destruction:** Trash disposal programs that provide for the secure disposal of sensitive trash (any discarded material that contains or could disclose confidential information). Such secure disposal of data, including without limitation electronic media, will be performed in a manner that practicably prevents the information from being read or reconstructed such as: (i) For paper documents, destruction with a crosscut shredder; and (ii) For electronic media, degaussing and physical destruction in accordance with NIST Special Publication 800-88.
Measures for ensuring events logging	Moosend has implemented procedures to maintain log activity in its Processing Environments, including: (a) Maintaining audit log events that identify a unique individual; (b) Maintaining audit logs showing all actions taken by any shared or generic user, such as administrator or root; (c) Protecting audit logs from unauthorized modification; (d) Audit logs must be promptly backed up to a central protected server; (e) Monitoring logs for security events, including intrusion detection or prevention system logs, perimeter and web application firewall logs; and (f) Taking steps so that all security events are promptly transmitted, investigated, and remediated by a security operations center.
Measures for ensuring system configuration, including default configuration	Moosend has implemented formal change control processes while making changes to its Processing Environments are maintained. These processes are designed to: (a) Provide a consistent approach for controlling and identifying changes in the Processing Environment. (b) Define roles and responsibilities in a manner that allows for appropriate segregation of duties, to prevent fraud and potential malicious or accidental misuse of the Processing Environment.

Measures for internal IT and IT security governance and management	Moosend maintains protocols to respond to any Security Incident in accordance with Customer requirements and pursuant to Data Protection Laws and Regulations: (a) **Security Incident Response Policy:** Moosend maintains a Security Incident Response Policy. This details: (i) Incident response workflow, including stakeholders in the Security Incident Response Team ("**SIRT**"); (ii) Risk assessment/classification criteria; (iii) Notification procedures; and (iv) Protocols for engaging and co-operating with relevant law enforcement agencies or forensic analysts. (b) **SIRT:** Moosend has a dedicated Security Incident Response Team to manage, respond and remediate to any security event or incident. (c) **SIRT Preparedness:** The SIRT will participate in regularly scheduled trainings to prepare for any Security Incident.
Measures for ensuring certification/assurance of processes and products.	See "Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services" above.
Measures for ensuring data minimisation	Moosend has implemented the following measures to store data on data media (manual or electronic) and for subsequent checking (e.g., database security, transmission security): (a) **Data segregation:** Procedures are maintained to prevent unauthorized access of Customer Data by providing dedicated hosting resources for Customer Data in its managed Processing Environment. This ensures that Customer Data is always separate from data belonging to other customers. (b) **DLP:** Data loss prevention controls are used to prevent the unauthorized transmission (e.g., email transmission) and inadvertent loss of Customer information (e.g., USB encryption, mobile device management).
Measures for ensuring data quality	Moosend has implemented the following measures to develop and implement secure software that has controls to protect the data that it stores and Processes: (a) **SDLC protocols:** Moosend maintains a secure software development standard policy, which covers training, requirements, design, implementation, verification, release and response to prevent and mitigate vulnerabilities in software creation. Some of the measures in the SDLC protocols include: (i) Maintaining logical network segmentation between production and non-production environments. (ii) Strictly controlling access to application source code and associated items (designs, specifications, and validations plans) for Moosend software to prevent the introduction of unauthorized functionality. (iii) Moosend access credential passwords used for production and non-production environments will be different. (iv) Moosend will not store Customer Data in non-production environments (development, testing, or staging environments). (v) Moosend must review all application code for security and/or coding vulnerabilities prior to production deployment in Moosend systems. Acceptable methods for code review include: (A) Static code testing tool (B) Dynamic code testing tool (C) Peer review (D) Tests must include coverage for: (E) Injection flaws (F) Buffer overflows (G) Insecure cryptographic storage (H) Improper error handling (I) Cross site scripting (J) Improper access controls (K) Cross-site request forgery (b) **Security implementation standards:** This includes ~~which include~~ security secure coding standards that address the OWASP Top 10 vulnerabilities within a testing environment prior to any external or Customer deployment. (c) **Penetration testing:** Moosend conducts penetration testing (performed by a third-party) prior to release, and after any significant change in how the software is managed in the Processing Environment.

	(i) Critical or High rated vulnerabilities must be addressed within 30 days of discovery. (ii) Medium rated vulnerabilities must be addressed within 90 days of discovery. (iii) Moosend will promptly notify Customer if it becomes aware of the software containing a zero-day vulnerability that presents a high risk to Customer Data and shall provide details on any appropriate mitigation strategy.
Measures for ensuring limited data retention	Moosend has implemented procedures (Records Retention and Disposal Policy) to securely retain then delete Customer Data upon termination of the applicable contract and physical destruction when applicable.
Measures for ensuring accountability	Moosend has implemented a data strategy to adapt to evolving security and Data Protection Laws and Regulations and has embedded robust data protection practices as part of our business culture. Strategic activities include: (a) Moosend has established an internal Data Governance Team to encourage centralized discussion of Moosend's strategic cross-functional privacy and security objectives, identify data governance risks and implement customer-oriented solutions. (b) The Data Governance Team is led by a Data Governance Committee (composed of Moosend's Executive leadership team) to ensure top-down advisory and management oversight, policy approval and appropriate awareness of privacy and security across all sectors of our organization. (c) When possible, we have set a global baseline for data-handling practices, following the most protective Data Protection Laws and Regulations, to ensure equal rights to privacy. (d) Privacy is built into services as part of our Software Secure Development Lifecycle. (e) Implementing strong security protocols, conforming to the highest international security standards, with policies and operational processes overseeing all aspects of our business practices, allowing us to ensure data protection throughout the data lifecycle. (f) Understanding that employees are our first line of defense, Moosend provides mandatory privacy, data protection and security training to all Moosend employees, consultants and contractors. (g) We want to be transparent with our customers, partners, service providers and web visitors about how we handle data in all your interactions with Moosend, and Process Personal Data only in accordance with specified instructions, as detailed in the Sitecore Privacy Policy. (h) Moosend's Privacy Team continuously reviews and monitors applicable Data Protection Laws and Regulations, trends and developments so that changes required by applicable laws, or which are appropriate to our business are made proactively.
Measures for allowing data portability and ensuring erasure	Moosend will support the right of return or deletion of data per section 8. Upon request, and apart from section 8, Customer may submit a request to receive a copy of their data.
Technical and organizational measures to be taken by the Data [sub]-processor to provide assistance to the Data Controller and, for transfers from a Data Processor to a Data [sub]-processor, to the Customer	Moosend maintains a vendor management process for the selection, oversight and risk assessment of third-party suppliers, vendors (including Subprocessors): (a) **Due diligence:** All new suppliers and vendors (including Subprocessors) must be procured in accordance with Moosend's Procurement Policy. This requires data review of privacy and security provisions by relevant stakeholders to assess and manage risk. (b) **Periodic assessments:** All existing suppliers and vendors (including Subprocessors) are subject to periodic assessment in accordance with Moosend's Procurement Policy. This requires data review of privacy and security provisions by relevant stakeholders to assess and manage risk.

ANNEX B
SUBPROCESSORS

Description
Moosend uses a range of third-party Subprocessors to assist it in providing the Services (as described in the Agreement).

Product-specific Subprocessors
The Subprocessors set out below are product-specific third-party Subprocessors, who provide cloud hosting services; application Processing services; database services; email sending/tracking services; as well as incident tracking, response, diagnosis, and resolution services.

Moosend		
Entity Name	**Description of the performance**	**Location**
AWS	Cloud Service Provider	Ireland and Germany
Microsoft	Microsoft Azure Services	Ireland and Germany
Neverbounce	Email list validation	USA

ANNEX C

DATA PROCESSING

The following is a description of the processing activities carried out by Moosend while acting as a Data Processor on behalf of the Customer, who is the Data Controller. Note that the exact nature of the categories of Personal Data of Processed using Moosend's product will depend on the Customer's usage of the products.

Definitions:

"Consumer": for the purposes of this description of processing a "Consumer" refers to "Data Subject" or "Data Subjects", as defined in the DPA, who consume the products or services offered by the Moosend Customer identified in the DPA and or the Agreement.
"User": This means a Moosend Customers' employee or authorized third party accessing Moosend's SaaS products.

List of Parties

Data Exporter		**Data Importer**	
Name:		Name:	Panos Melissaropoulos
Address / Email Address: As provided for in the DPA:		Address / Email Address: As provided for in the DPA:	10 Eastbourne Terrace, London, United Kingdom, W2 6LG
Contact Person's Name, position and contact details: As provided for in the DPA:		Contact Person's Name, position and contact details: As provided for in the DPA:	Vice President, *official signatory on behalf of Moosend LTD*
Activities Relevant to the Transfer		Activities Relevant to the Transfer	
Role (Data Controller/Data Processor):	Data Controller	Role (Data Controller/Data Processor):	Data Processor

Categories of Data Subjects	Consumer, User
Categories of Users' Personal Data Processed	• Contact Information (e.g., name, email) • Account and Authentication Data (e.g., username, passwords, session tokens) • Usage Data (e.g., device IDs, performance and network logs, IP addresses for security) • Behavioural - Information that describes a User's behaviour or activity, captured through Users operation of Moosend Products • Location data - Geolocation data, country, region, time zone captured through User's operation of Moosend Products.
Categories of Consumers' Personal Data Processed	• Contact Information (e.g., name, phone number, email, username) • Account and Authentication Data (e.g., passwords, session tokens) • Usage Data (e.g., device IDs, performance and network logs, IP addresses for security) • Behavioural - Information that describes a Consumer's behaviour or activity, captured through Consumer's engagement with Customer's deployment of Moosend's product(s). • Preference - Information about a Consumer's preferences or interests, opinions, intentions, captured through Consumer's engagement with Customer's deployment of Moosend's product(s). Transactional – Information about a Consumer's purchases of Customers product(s) and/or service(s) captured through Consumer's engagement with Customer's deployment of Moosend's product(s). • Location data- Geolocation data, country, region captured through Consumer's engagement with Customer's deployment of Moosend's product(s).
Data Controller/ Data Processor roles	Moosend is Data Processor, Customer is the Data Controller

Special Category Data Processing	Moosend does not knowingly collect (and Customer or Users shall not submit or upload) any special categories of data (as defined under applicable Data Protection Laws and Regulations).
Nature of the Processing	• Use of Personal Data to set up, operate, monitor, and provide the Services • Storage of Personal Data in dedicated data centers. • Back up and restoration of Personal Data stored in the dedicated data centers and Cloud Service. • Computer Processing of Personal Data, including data transmission, data retrieval, data access. • Network access to allow Personal Data transfer. • Monitoring, troubleshooting, and administering the underlying Cloud Service infrastructure and database. • Security monitoring, network-based intrusion detection support, penetration testing. • Execution of instructions of Customer in accordance with the Agreement. • Deletion and disposal of Customer Data
Purpose of the data Processing	• **supporting and enabling Moosend's services** for the Customer, in accordance with their specific instructions, while ensuring **data security, integrity, and availability**.
Duration of Processing	Moosend will Process Customer Data for the duration of the Agreement, unless otherwise agreed upon in writing with the Customer.

ANNEX D

MECHANISMS FOR PERSONAL DATA TRANSFERS

The Parties have agreed on the following Data Transfer Mechanisms in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the Personal Data specified in Appendix 1.

For the purposes of Article 46 (2) of Regulation 2016/679 for the transfer of Personal Data to Data Processors established in third countries which do not ensure an adequate level of data protection, the Standard Contractual Clauses are the adequate transfer mechanism.

For transfers of Personal Data in compliance with section 119A and article 46 of the Data Protection Act 2018, the Parties agree that the Standard Contractual Clauses supplemented by the UK International Data Transfer Addendum are the appropriate transfer mechanism.
For transfers of Personal Data in compliance with the Federal Act on Data Protection 1992 ("**FADP**"), the Parties agree that the Standard Contractual Clauses supplemented by the Swiss Addendum to the EU Commission Standard Contractual Clauses are the appropriate transfer mechanism.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) [(1)] for the transfer of Personal Data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the Personal Data, as listed in Annex I.A (hereinafter each 'Data Exporter'), and

(ii) the entity/ies in a third country receiving the Personal Data from the Data Exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'Data Importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of Personal Data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable Data Subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of Data Subjects.

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

Clause 3

Third-party beneficiaries

(a) Data Subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the Data Exporter and/or Data Importer, with the following exceptions:

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

(Intentionally left blank)

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The Data Exporter warrants that it has used reasonable efforts to determine that the Data Importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The Data Importer shall process the Personal Data only on documented instructions from the Data Exporter. The Data Exporter may give such instructions throughout the duration of the contract.

(b) The Data Importer shall immediately inform the Data Exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The Data Importer shall process the Personal Data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the Data Exporter.

8.3 Transparency

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

8.4 Accuracy

If the Data Importer becomes aware that the Personal Data it has received is inaccurate, or has become outdated, it shall inform the Data Exporter without undue delay. In this case, the Data Importer shall cooperate with the Data Exporter to erase or rectify the data.

8.5 Duration of Processing and erasure or return of data

Processing by the Data Importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the Processing services, the Data Importer shall, at the choice of the Data Exporter, delete all Personal Data processed on behalf of the Data Exporter and certify to the Data Exporter that it has done so, or return to the Data Exporter all Personal Data processed on its behalf and delete existing copies. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Data Importer that prohibit return or deletion of the Personal Data, the Data Importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the Data Importer under Clause 14(e) to notify the Data Exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of Processing

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

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

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

(d)The Data Importer shall cooperate with and assist the Data Exporter to enable the Data Exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected Data Subjects, taking into account the nature of Processing and the information available to the Data Importer.

8.7 Sensitive data

Where the transfer involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the Data Importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The Data Importer shall only disclose the Personal Data to a third party on documented instructions from the Data Exporter. In addition, the data may only be disclosed to a third party located outside the European Union [4] (in the same country as the Data Importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

(a)The Data Importer shall promptly and adequately deal with enquiries from the Data Exporter that relate to the Processing under these Clauses.

(b)The Parties shall be able to demonstrate compliance with these Clauses. In particular, the Data Importer shall keep appropriate documentation on the Processing activities carried out on behalf of the Data Exporter.

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

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

The Data Importer has the Data Exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The Data Importer shall specifically inform the Data Exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fourteen (14) days' in advance, thereby giving the Data Exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The Data Importer shall provide the Data Exporter with the information necessary to enable the Data Exporter to exercise its right to object.

(b)Where the Data Importer engages a sub-processor to carry out specific Processing activities (on behalf of the Data Exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the Data Importer under these Clauses, including in terms of third-party beneficiary rights for Data Subjects. [8] The Parties agree that, by complying with this Clause, the Data Importer fulfils its obligations under Clause 8.8. The Data Importer shall ensure that the sub-processor complies with the obligations to which the Data Importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data Subject rights

(a)The Data Importer shall promptly notify the Data Exporter of any request it has received from a Data Subject. It shall not respond to that request itself unless it has been authorised to do so by the Data Exporter.

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

(c)In fulfilling its obligations under paragraphs (a) and (b), the Data Importer shall comply with the instructions from the Data Exporter.

Clause 11

Redress

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

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

(c)Where the Data Subject invokes a third-party beneficiary right pursuant to Clause 3, the Data Importer shall accept the decision of the Data Subject to:

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

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

[Where the Data Exporter is not established in an EU Member State, but falls within the territorial scope of application of

Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the Data Subjects whose Personal Data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards [(12)];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the Processing of the Personal Data in the country of destination.

(c) The Data Importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the Data Exporter with relevant information and agrees that it will continue to cooperate with the Data Exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

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

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

Clause 15

Obligations of the Data Importer in case of access by public authorities

15.1 Notification

(a) The Data Importer agrees to notify the Data Exporter and, where possible, the Data Subject promptly (if necessary, with the help of the Data Exporter) if it:

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)The Data Importer shall promptly inform the Data Exporter if it is unable to comply with these Clauses, for whatever reason.

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

(c)The Data Exporter shall be entitled to terminate the contract, insofar as it concerns the Processing of Personal Data under these Clauses, where:

(i)the Data Exporter has suspended the transfer of Personal Data to the Data Importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii)the Data Importer is in substantial or persistent breach of these Clauses; or

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

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

(d)Personal Data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the Data Exporter immediately be returned to the Data Exporter or deleted in its entirety. The same shall apply to any copies of the data. The Data Importer shall certify the deletion of the data to the Data Exporter. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred Personal Data, the Data Importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A Data Subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

On behalf of the Data Importer:	**Moosend LTD.**
Name (written out in full):	Panos
Position:	Vice President
Address:	10 Eastbourne Terrace London United Kingdom W2 6LG
Other information necessary in order for the contract to be binding (if any):	*Not applicable*
Signature	

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses between the Data Exporter and Data Importer (and its Affiliates) and must be completed and signed by the parties.

Name of the data exporting organisation: Customer

Name:	
Authorised Signature:	

Name of the data importing organisation: Moosend

Name:	Panos Melissaropoulos
Authorised Signature:	

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

Please refer to **Annex C** of the Customer Data Processing Addendum for description of transfer.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix must be completed and signed by Data Exporter and Data Importer.

Name of the data exporting organisation: Customer

Name:	
Authorised Signature:	

Name of the data importing organisation: Moosend

Name:	Panos Melissaropoulos
Authorised Signature:	

Please refer to **Annex A** of the Customer Data Processing Addendum for a description of the technical and organisational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c).

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

This Addendum amends the Standard Contractual Clauses to the extent necessary so they operate for transfers made by the Data Exporter to the Data Importer, to the extent that section 119A(1) of the Data Protection Act 2018 ("**DPA 2018**") applies to the Data Exporter's Processing when making that transfer.

Part 1: Tables with Parties' Information

Table 1: Parties and Signatures

Start Date	
The Effective Date of the Agreement	
The Parties	
Exporter (who sends the Restricted Transfer)	
Full Legal Name	
Main address (if a company registered address):	
Official registration number (if any) (company number or similar identifier):	
Key Contact (Full Name, Job Title, Email)	
Importer (who receives the Restricted Transfer)	
Full Legal Name	Moosend LTD
Main address (if a company registered address):	10 Eastbourne Terrace, London, United Kingdom, W2 6LG
Official registration number (if any) (company number or similar identifier):	
Key Contact (Full Name, Job Title, Email)	
Signature (if required for the purposes of Section 2)	
Exporter (who sends the Restricted Transfer)	
Importer (who receives the Restricted Transfer)	

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: Module Two, as set out in Annex D to the DPA.			☒			
			Date:	The Effective Date of the Agreement		
			Reference (if any):	Not applicable		
			Other Identifier (if any):	Not applicable		
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.	Module Two	Not applicable	Not applicable	General Authorisation	14 Days	Not applicable

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 set out in Annex C to the DPA
Annex 1B: Description of Transfer:	As set out in Annex C to the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	As set out in Annex A to the DPA
Annex III: List of Sub processors:	As set out in Annex B 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 19:	
	Importer	☒
	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 Safeguards	The standard of protection over the Personal Data and 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 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.

Swiss Addendum to the EU Commission Standard Contractual Clauses

This Addendum amends the Standard Contractual Clauses to the extent necessary so they operate for transfers made by the Data Exporter to the Data Importer, to the extent that the Federal Act on Data Protection 1992 ("**FADP**") applies to the Data Exporter's processing when making that transfer.

The Standard Contractual Clauses shall be amended with the following modifications:

The Swiss Federal Data Protection and Information Commissioner (the "**FDPIC**") will be the competent supervisory authority, in Annex D under Clause 13 of the SCCs;
The applicable law for contractual claims and place of jurisdiction for actions between the parties under Clauses 17 and 18 of the Standard Contractual Clauses shall be as set forth in the Standard Contractual Clauses, provided that that the term "member state" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual reside (Switzerland) in accordance with Clause 18(c).;
References to the "GDPR" should be understood as references to the "FADP;" and
Where the FADP protects legal entities as Data Subjects, the SCCs will apply to data relating to identified or identifiable legal entities.