NOTICE: Please review our updated Data Processing Addendum, which details how we handle personal information in accordance with applicable privacy laws.

DATA PROCESSING ADDENDUM

Last Updated: June 2025

This Data Processing Agreement (this "DPA") is between Moosend (as defined below), and the Moosend customer or trialer agreeing to the Moosend Terms and Conditions (the "Terms and Conditions") (such customer or trialer, the "Customer"). This DPA supplements and forms part of the Terms and Conditions. If a term is capitalized in this DPA but not defined, it has the meaning given to it in the Terms and Conditions. This DPA governs the terms under which Moosend will Process Customer Personal Data (each as defined below) on behalf of Customer. In the event of any conflict or discrepancy between the Terms and Conditions and this DPA, this DPA shall prevail. In the event of any conflict or discrepancy between this DPA and the Standard Contractual Clauses, as applicable, the Standard Contractual Clauses shall prevail.

The parties to this DPA hereby agree to be bound by the terms and conditions herein, as applicable, with effect from the date Customer accepted the Terms and Conditions (the "Effective Date"). Moosend may amend this DPA from time to time due to changes in Data Protection Laws or as otherwise determined by Moosend in its commercially reasonable discretion. Any amendment will only become effective upon notification to Customer (by email or by posting on Moosend's website) and, if Customer does not agree to any such amendment, it should stop using the Services and contact Moosend to cancel Customer's account.

Under the Terms and Conditions, Customer has engaged Moosend to provide Services to Customer. As a result of its providing the Services to Customer, Moosend will store and process certain personal information of Customer as described below:

1. Definitions.   For purposes of this DPA, the following capitalized terms shall have the meanings indicated below. Whenever the words "include", "includes" or "including" are used in this DPA, they shall be deemed to be followed by the words "without limitation".

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Controller" means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. The definition of Controller includes “Business” as that term is defined by the CCPA.

“**Customer Personal Data**” means Personal Data provided by Customer to Moosend for Processing on behalf of Customer pursuant to the Terms and Conditions.

“**Data Protection Laws**” means, with respect to a party, all laws and regulations of the relevant jurisdictions that apply to such party’s performance of obligations and exercise of rights under this DPA, including the Regulation (EU) 2016/679 of 27 April 2016, General Data Protection Regulation (the “GDPR”), the California Consumer Privacy Act (the “CCPA”), as amended by the California Privacy Rights Act (the “CPRA”), Brazil’s Lei Geral de Proteção de Dados Pessoais (“LGPD”), and other U.S. federal or state data privacy and data protection laws, and related implementing regulations.

“**Data Subject**” means the identified or identifiable person to whom Personal Data relates. The definition of Data Subject includes “Consumer” as that term is defined by the CCPA.

“Moosend” means Moosend, Ltd.

“**Personal Data**” means any information relating to a Data Subject.

“**Process**”, “**Processed**” or “**Processing**” means any operation or set of operations that is or are 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.

“**Processor**” means a natural or legal person, public authority, agency or other body that Processes Customer Personal Data on behalf of the Controller. The definition of Processor includes “Service Provider” as that term is defined by the CCPA.

“**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 of the Council, and implemented by the European Commission decision 2021/914, dated 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj.

“**Sub-processor**” means any Processor engaged by Moosend or its Affiliates in connection with provision of the Services.

2. Processing of Personal Data

(a) **Roles of the Parties.** The parties acknowledge and agree that with regard to Processing of

Personal Data, Customer is either a Controller or a Processor and that Moosend is a Processor.

(b) **Customer Obligations**. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws, including that it shall have (i)obtained any necessary consents or provided any necessary notices, including notices to Data Subjects of the use of Moosend as Processor (including where Customer is a Processor, by ensuring that the ultimate Controller does so), and (ii) a legitimate ground to disclose Customer Personal Data to Moosend and enable the Processing of Customer Personal Data by Moosend as set out in this DPA and as contemplated by the Terms and Conditions. Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject, including those that have opted-out from marketing or other disclosures of Personal Data, to the extent applicable under Data Protection Laws.

(c) **Moosend's Processing of Personal Data**. Moosend shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Terms and Conditions; (ii) Processing initiated by individuals in their use of the Services (including any configuration of or use of any settings, features, or options in the Services by any individual acting on behalf of Customer); and (iii) Processing to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with this DPA and the Terms and Conditions. If Moosend becomes aware that any instruction by Customer violates Data Protection Laws, Moosend agrees to inform Customer of its inability to comply as soon as reasonably practicable at the email address provided by Customer to Moosend. Moosend shall not be liable for any claim brought by Customer or a Data Subject arising from any action or omission by Moosend to the extent that such action or omission resulted from Customer's instructions or breach of this DPA.

(d) **Details of Processing**. The subject matter of the Processing of Personal Data under this DPA is the provision of Services pursuant to the Terms and Conditions. The duration of the Processing, the nature and purpose of the Processing, the categories of Data Subjects and the types of Personal Data Processed pursuant to this DPA are set forth on Annex I attached hereto.

3. Moosend Personnel. Moosend shall ensure that its personnel who are authorized to Process Customer Personal Data have received appropriate training on their responsibilities and are subject to confidentiality obligations.

4. Security. Moosend shall implement and maintain during the term of this DPA appropriate technical and organizational security measures to protect the security of Customer Personal Data as further detailed in Annex II.

5. Data Subject Rights. Upon receipt by Moosend of a written request from an individual seeking to exercise any of their rights under Data Protection Laws related to Customer Personal Data, Customer authorizes Moosend to direct such individual to Customer. Taking into account the nature of the Processing, Moosend shall, at Customer's expense, assist Customer by appropriate technical and organizational measures, for the fulfillment of Customer's obligation to respond to requests by Data Subjects to exercise their rights under Data Protection Laws (including, as applicable, the data subject access right, the right to rectification and erasure, the right to the restriction of processing, the right to data portability and the right to object to processing). Moosend shall carry out a request from Customer to amend or correct any of Customer Personal Data to the extent necessary to allow Customer to comply with its responsibilities under Data Protection Laws. Further, Moosend shall carry out a request from Customer to block, transfer or delete any of Customer Personal Data to the extent necessary to allow Customer to comply with its responsibilities as a Controller, in each case unless otherwise permitted or required by Data Protection Laws.

6. Cooperation. Taking into account the nature of the Processing under the Terms and Conditions and the information available to Moosend, Moosend shall, insofar as commercially practicable and at Customer's expense, assist Customer in carrying out its obligations under Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators. Moosend shall promptly notify Customer about any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data, as required by Data Protection Laws.

7. Return and Deletion of Customer Personal Data. Upon termination of the Processing of Customer Personal Data by Moosend and at the written request of Customer, Moosend shall either (i) delete all Customer Personal Data, or (ii) return all Customer Personal Data to Customer and delete existing copies, in each case unless otherwise permitted or required by Data Protection Laws.

8. Audits. Customer may request that Moosend provide a certification or summary of an audit report that demonstrates compliance with its obligations under this DPA or Data Protection Laws. If such information is not reasonably sufficient to prove Moosend's compliance with Data Protection Laws, Moosend shall, subject to reasonable advance notice and during normal business hours, permit Customer or an independent third party authorized by Customer and that is not a competitor of Moosend, to carry out the audits and inspections of the processing of Customer Personal Data by the Moosend. Moosend may require the third to enter into a confidentiality agreement before permitting it to carry out an audit or inspection. Moosend shall not be responsible for any costs or expenses relating in connection with any audit or inspection contemplated by this Section 8. The auditing party shall bear its own costs in relation to such an audit. The obligations set forth in this Section 8 shall only apply to Moosend to the extent required by Data Protection Laws.

9. International Data Transfers.

(a) It is acknowledged and agreed by Customer that Moosend, in providing the Services under the Terms and Conditions, transfers Customer Personal Data to its servers in the United States and anywhere else in the world where Moosend, its Affiliates and its Sub-processors maintain data processing operations.

(b) **Standard Contractual Clauses.**

(i) If applicable, transfers of Customer Personal Data will be under the Standard Contractual Clauses and the relevant UK Addendum to the clauses. If Customer acts as a Controller, then Module 2 of the Standard Contractual Clauses shall apply. If Customer acts as a Processor for Customer Personal Data, then Module 3 of the Standard Contractual Clauses shall apply. The following terms in this Section shall apply to the Standard Contractual Clauses:

(1) Annexes I, II and III to this DPA shall be deemed automatically incorporated into Annexes I, II and III of the Standard Contractual Clauses;
(2) Section 1, Clause 7 of the Standard Contractual Clauses is intentionally omitted;
(3) For the purposes of Section 2, Clauses 8.9(c) and (d) of the Standard Contractual Clauses, audits will be performed in accordance with Section 8 of this DPA;
(4) For the purposes of Section 2, Clause 9 of the Standard Contractual Clauses, Customer consents to Moosend appointing Sub-processors in accordance with Section 12 of this DPA;
(5) For the purposes of Section 2, Clause 17, the governing law shall be the laws of the Republic of Ireland; and
(6) For purposes of Section 2, Clause 18, the courts shall be the courts of the Republic of Ireland.

(ii) With respect to transfers to which the UK Data Protection Laws apply, the Standard Contractual Clauses shall apply and shall be deemed amended as specified by the UK Addendum attached hereto as Annex IV.

(iii) For data transfers governed by Swiss data protection laws, general and specific references in the Standard Contractual Clauses to “GDPR” or “EU” or “Member State Law” shall have the same meaning as the equivalent reference in Swiss data protection laws.

10. Indemnification. Customer agrees that it will indemnify and hold harmless Moosend and its Affiliates on demand from and against all claims, liabilities, costs, expenses, loss or damage (including consequential losses, loss of profit and loss of reputation and all interest, penalties and legal and other professional costs and expenses) incurred by Moosend arising directly or indirectly from a breach of this DPA or any Data Protection Laws.

11. Sub-Processing

(a) Customer acknowledges and agrees that Moosend may retain an Affiliate or third party subcontractor as Sub-processors. Moosend has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in this DPA with respect to the protection of Customer Personal Data to the extent applicable to the nature of the services provided by such Sub-processor.

(b) Moosend shall maintain a list of its Sub-processors at https://moosend.com/wp-content/uploads/2025/01/SUBPROCESSORS-MOOSEND.pdf, which will be updated from time to time to reflect any change in Sub-processors.

12. Termination. Termination of this DPA shall be governed by the Terms and Conditions, mutatis mutandis.

13. Law and Jurisdiction

This DPA will be governed by English law without regard or reference to its principles of conflicts of laws, and each party hereby submits to the exclusive jurisdiction of the English courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): The data exporter is Customer. Customer acts as a Controller or Processor.

Data importer(s): The data importer is Moosend, which acts as a Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Customer Personal Data transferred concerns Customer's customers, contacts, prospective customers, and website visitors.

Categories of personal data transferred: As applicable, name, contact information (e.g., email address, phone number, physical address), geographical data, device identification data, information from connected accounts authorized by Customer, and other Customer Personal Data processed pursuant to the Terms and Conditions. Depending on how Customer uses the Services, the following information could be inferred from Customer's usage: business network and experience, educational data, financial data, and interests.

Sensitive data transferred (if applicable): The parties do not anticipate special categories of data being processed. Depending on how Customer uses the Services, some sensitive data may be inferred from Customer's Usage.

The frequency of the transfer: Personal Data will be transferred on a continuous basis.

Nature of the processing: Customer determines the types of data they submit to Moosend to process on their behalf in the course of using the Services pursuant to the Terms and Conditions.

Purpose(s) of the data transfer and further processing: Personal Data shall be processed to provide the Services to Customer.

The period for which the personal data will be retained: Data Processing will be for the term of the Terms and Conditions and for a reasonable period of time after the termination of the Terms and Conditions.

For transfers to (sub-) processors: Moosend may engage Sub-processors to provide parts of the Services in compliance with the parties' agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Irish Data Protection Commission.

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

(See following page)

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) **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. (c) **Processes:** Moosend maintains several policies, including an Information Security Policy, designed to maintain consistent controls while governing Moosend's security program. (d) **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. (e) **Policies:** Moosend shall upgrade and in no way degrade controls from that stated on the Privacy and Security Page. (f) **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. (g) **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) 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 III

LIST OF SUB-PROCESSORS

Customer has authorized the use of the Sub-processors detailed at https://moosend.com/wp-content/uploads/2025/01/SUBPROCESSORS-MOOSEND.pdf, which are applicable to the Services being provided to Customer.

ANNEX III
UK ADDENDUM

International Data Transfer Addendum Addendum to the EU Commission Standard Contractual Clauses

For purposes of this UK Addendum to Schedule 1 (the "UK Addendum"), capitalized terms used but not defined herein shall have the meaning set forth in either Addendum or the UK Data Protection Act 2018, as applicable.

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

Part 1: Tables

Table 1: Parties

Start date	Effective Date as defined in the attached Data Processing Addendum ("DPA").

The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**

Parties' details	Full legal name: Customer Trading name (if different): N/A Main address (if a company registered address): As designated in Customer's account Official registration number (if any) (company number or similar identifier): N/A	Full legal name: Moosend, Ltd. Trading name (if different): N/A Main address: 5 New Street Square, London, United Kingdom, EC4A 3TW Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): Customer Job Title: N/A Contact details including email: As designated in Customer's account	Full Name (optional): Job Title: General Counsel Contact details including email: privacy@moosend.com
Signature (if required for the purposes of Section 2)	Exporter is deemed to have signed this UK Addendum as of Effective Date as defined in the DPA.	Importer is deemed to have signed this UK Addendum as of the Effective Date as defined in the DPA.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Effective Date as defined in the DPA

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: See Table 1 of this UK Addendum

Annex 1B: Description of Transfer: See Annex 1B of the Standard Contractual Clauses

Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: See Annex II of the Standard Contractual Clauses

Annex III: List of Sub processors (Modules 2 only): See Annex III of the Standard Contractual Clauses

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

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.