SPECIAL PART OF THE SERVICE CONTRACT

Joint Stock Company Lietuvos paštas, a joint stock company legally registered and operating under the laws of the Republic of Lithuania, legal entity code 121215587, VAT payer code LT212155811, registered office address J. Jasinskio g. 16, LT-03500 Vilnius, Republic of Lithuania, the data of which are collected and stored by the State Enterprise Centre of Registers. represented by the Director of the Business Development and Technology Department, , acting in accordance with the order No. 1-2021-00001 of 4 January 2021 of the Director General of the Joint Stock Company Lietuvos paštas (hereinafter — the Buyer), and

MailerLite Limited, a private limited company legally registered and operating under the laws of the Republic of Ireland, legal entity number 689826, VAT number IE3748416JH, registered office at Ground Floor, 71 Lower Baggot Street, Dublin 2 D02 P593, Ireland, the particulars of which are held by the Companies Registration Office of Ireland, represented by the Director, (hereinafter — the Service Provider),

The Buyer and the Service Provider, each individually hereinafter referred to as a Party and collectively referred to as the Parties, have entered into this Service Contract (hereinafter — the Contract).

1. GENERAL PROVISIONS AND OBJECT OF THE CONTRACT

1.1. The Service Provider undertakes to provide the Buyer with the email system services (hereinafter — the Services) on the terms and conditions set out in the Contract and the Buyer undertakes to pay for the Services on the terms and conditions set out in the Contract.

1.2. This Contract is the result of a public procurement procedure in which the most economically advantageous tender was selected based on price.

1.3. The Contract GP is an integral part of this Contract. The Contract GP is available at https://www.post.lt/lt/viesieji-pirkimai. In the event of any conflict between the published Contract GP and the Contract GP referred to in the documents of the public procurement based on which this Contract was concluded, the latter shall prevail.

1.4. For the interpretation and application of the Contract, Clause 2.1 of the GP sets out the order of precedence of the Contract Documents.

2. SCOPE AND PRICE OF SERVICES

2.1. The services to be provided to the Buyer under this Contract shall be the email system services described in the Technical Specification (Annex to Contract GP No. 2).

2.2. The Contract is priced on a fixed-fee basis. Services are purchased based on customer demand.

2.3. The total price of the Services shall be EUR *4,863.60 (four thousand eight hundred and sixty-three* euros and *sixty* ct), including VAT. The total price of the Services shall be:

2.3.1. EUR *4,863.60 (four thousand eight hundred and sixty-three* euros *and sixty* ct) excluding VAT;

2.3.2. No value added tax is levied in accordance with Article 13(2) of the Law of the Republic of Lithuania on Value Added Tax.

2. SERVICE QUALITY

3.1. The quality of the Services shall be in accordance with the attached Technical Specification or other documents that set out the quality requirements for the Services.

3.2. For defects in the output of the Template Upload Services identified by the Buyer and for technical glitches in the email parameters, other than those referred to in Clause 3.3 of the Contract, a time limit of *2 working days* shall be set from the date of notification of the defect or glitch.

3.3. The remedy for the shortcomings of particular urgency is the disruption of the delivery of the report and the disruption of the dispatch of letters provided for in Clause 5.1 of the Technical Specification. These disruptions must be rectified within *1 working day* from the date of notification of the disruption.

3.4. In the event of any doubt by the Buyer as to the quality of the Services, the Parties may commission an examination. The terms of the examination are set out in Clause 6.8 of the Contract GP.

3.5. During the term of the Contract, the Service Provider undertakes to take measures to conserve natural resources and to comply with the following environmental requirements: reduce paper consumption, avoid

unnecessary copying and printing of documents. If stationery is to be used for the service, it must be recycled or recyclable (the Service Provider must keep documentation proving the characteristics of the goods). VAT invoices and/or other documents relating to the performance of the Contract shall be submitted to the Buyer only in electronic format.

4. RELYING ON THE CAPACITIES OF OTHER ECONOMIC OPERATORS

4.1. The contract is carried out on the Service Provider's side based on joint activities: NO

4.2. Where the Service Provider has relied on the economic and financial capacities of other economic operators in the course of the Procurement Procedures to demonstrate compliance with the requirements set out in the Conditions of Contract, the Service Provider and the economic operators whose capacities the Service Provider has relied on shall be jointly and severally liable for the performance of the Contract.

4.3. The Service Provider shall have the right to use Subcontractors for the performance of the Contract only for the part of the Contract specified in the Tender. The Service Provider has indicated in the Tender the part of the Contract for which Subcontractors will be used: NO.

5. TIME LIMITS FOR THE PROVISION OF SERVICES, PROCEDURES FOR THE HANDOVER AND ACCEPTANCE OF THE RESULT OF THE SERVICE

5.1. The Service Provider undertakes to provide the Services described in the Technical Specification in accordance with the Contracting Authority's actual needs and deadlines.

5.2. The start of use of the system is specified in Clause 2.3 of the Technical Specification (by the date specified, the Service Provider shall create a master user (if required), and provide logins or other necessary information to the Buyer).

5.3. There shall be a time limit of 2 working days within which the Buyer shall either accept the Services provided (uploading of the template into the system) or inform the Service Provider in writing of any deficiencies in the result of the Services (the time limit for the correction of deficiencies is set out in Clause 3.2).

5.4. For delay in providing the Services within the time limit set out in Clause 5.1 of the Technical Specification and/or in rectifying deficiencies within the time limits set out in Clauses 3.2 and 3.3 of the Contract SP, the Service Provider shall pay to the Buyer, at the Buyer's request, a penalty of EUR 10 (ten euros) for each day of delay (but in any case not less than EUR 50.00 (fifty euros) for the whole period of delay).

6. PAYMENTS, MONETARY OBLIGATIONS, AND RETENTIONS

6.1. The Buyer shall pay to the Service Provider the monthly Service Fee for the Services rendered during the preceding calendar month within 30 (thirty) calendar days of receipt of the Invoice.

6.2. The maximum amount of liquidated damages and/or penalties payable by the Service Provider under this Contract shall not exceed the total price of the Services as set out in Clause 2.3 of the Contract SP.

6.3. The Buyer reserves the right to suspend payment for the Services if there are uncorrected deficiencies in the provision of the Services until all deficiencies have been corrected. Payments to the Service Provider may be suspended if the invoice submitted contains an incorrect amount or scope.

6.4. Payment for the Services shall be deemed to be made on the date on which the Buyer's bank debits the amount payable from the Buyer's bank account. The Buyer shall not be liable and the Buyer shall not be deemed to be in breach of the payment terms set out in this Contract if funds debited from the Buyer's bank account for payment for the Services are withheld for any reason (e.g., in connection with the prevention of money laundering and terrorist financing) or returned to the Customer by any bank or correspondent for reasons unrelated to the Customer.

6.5. The Buyer may at any time verify the Service Provider's compliance with Clause 3.5 of this Contract by requesting a report or by inspecting the Service Provider during the performance of the Services, and a fine of EUR 100 shall be imposed in the event of a failure to comply with this requirement.

7. ENTRY INTO FORCE AND VALIDITY OF THE CONTRACT

7.1. This Contract shall enter into force upon signature by the Parties and shall remain in force until the Parties' contractual obligations have been fully performed. The Services are provided for 12 months. Commencement of Services shall be no earlier than 9 September 2022.

7.2. Upon expiry of the Contract, the Service Provider shall provide the Buyer with the details of customers who have opted out of the newsletters. The Service Provider will also be required to delete all existing databases. The termination of the Contract shall not affect those obligations arising out of the Contract which, by their nature and substance, shall survive its termination.

8. SPECIAL TERMS

8.1. The Parties shall sign a confidentiality agreement in accordance with Clause 13.8 of the Contract GP in the form provided by the Buyer (Annex to Contract GP No. 4). This Agreement is a prerequisite for the entry into force of the Contract.

8.2. The Service Provider confirms that the circumstances resulting from the unfavourable epidemiological situation caused by the coronavirus infection (COVID-19) caused by the decisions of the competent state and/or municipal authorities of the Republic of Lithuania or of other countries, which impose restrictions on the movement of persons and/or economic activities, shall not be considered as force majeure and shall not relieve the Service Provider of its liability for the non-performance of the contract.

8.3. The Parties have agreed that if new circumstances arise after the conclusion of the Contract which restrict the activities of the Service Provider to a greater extent or in a different manner than known at the time of the conclusion of the Contract and which prevent the Service Provider from fulfilling its contractual obligations, then the Service Provider may be relieved of its civil liability for non-performance, only if the Service Provider proves that the circumstances relied on by the Service Provider are of such a magnitude and nature that no prudent and careful businessman could have controlled and foreseen at the time of the conclusion of the contract and that the Service Provider could not, by the exercise of due diligence, have prevented the occurrence of the circumstances or their consequences.

8.4. If the Service Provider is unable to perform its obligations under the Contract, it must submit a request to the Buyer in accordance with the procedure set out in the Contract, including details of the specific unforeseen circumstances (e.g., restrictions on the company's activities, governmental bans on the export of the goods concerned, etc.), and the reasons for the unforeseeable disruption of the Contract, which the Service Provider was not able to foresee at the time of conclusion of the Contract. In order to be exempted from civil liability, the Service Provider must provide all the information requested by the Buyer and specified in the contract, together with the documents supporting this information.

8.5. Corruption of any kind is not tolerated. The Buyer shall have the right to unilaterally terminate the Contract if the Service Provider (including any of the Service Provider's employees, agents, subcontractors, representatives and others) gives or offers (directly or indirectly) to any of the Buyer's employees, any benefit in the form of an item of property, gratuity, commission, services or other tangible or intangible benefit as an inducement or reward for doing or refraining from doing any act in connection with this Contract or for showing or refraining from showing favouritism or disfavour to any person in connection with this Contract (a bribe). In the event of termination of the Contract by the Buyer on this basis, the Service Provider shall reimburse the Buyer for all costs incurred by the Buyer in completing the performance of the Contract and shall indemnify the Buyer for all losses incurred as a result of the termination of the Contract.

8.6. If the Service Provider is unable to perform its obligations under the Contract, it must submit a request to the Buyer in accordance with the procedure set out in the Contract, including details of the specific unforeseen circumstances (e.g., restrictions on the company's activities, governmental bans on the export of the goods concerned, etc.), and the reasons for the unforeseeable disruption of the Contract, which the Service Provider was not able to foresee at the time of conclusion of the Contract. In order to be exempted from civil liability, the Service Provider must provide all the information requested by the Buyer and specified in the contract, together with the documents supporting this information.

8.7. The Parties agree that the Buyer shall have the right to unilaterally terminate any or all of its contracts with the Service Provider immediately, without any penalty, indemnity, compensation or refund to the Service Provider and/or its subcontractor, and that the Buyer may cancel any or all Orders and/or suspend the performance, in whole or in part, of any of its contracts with the Service Provider, in the event of economic or other international sanctions being imposed on the Service Provider and/or its ultimate beneficiary (i.e., a natural person who, directly and/or indirectly, acting alone or jointly with other persons, is the ultimate owner of the Service Provider and/or controls and/or exercises control or direction over the Service Provider and/or its management) and/or any natural or legal person related to the recipient and/or the recipient and/or its beneficiary. In the event of any conflict between the provisions of this Clause and the provisions of Clause 3.6 of the Contract GP, the provisions of this Clause shall prevail. If the failure or improper performance by the Service Provider of its obligations under the Contract results in the Buyer being subject to fines, penalties, etc., imposed by the competent authorities (e.g., the Buyer being obliged to carry out certain actions, etc.), the Service Provider shall be liable to indemnify the Buyer for any damages suffered by the Buyer as a result thereof.

8.8. As the Buyer and its relations with third parties are subject to the Resolution of the Board of the Bank of Lithuania No. 03-174 of 26 November 2020 “On the Approval of the Description of Information and Communication Technologies and Security Risk Management Requirements”, the Service Provider undertakes to provide training to its own employees, and if it uses third parties (e.g., subcontractors), to provide training in the field of information security and related areas to reduce the incidence of human error, theft, fraud, abuse, or loss, and to eliminate the risk of security risks in those areas. This training must be carried out

at least once a year. The Service Provider shall immediately inform the Buyer if additional information is required for this training. The Service Provider shall promptly provide information on the provision of such training upon request by the Buyer.

8.9. The Parties have agreed that the Buyer shall have the right to unilaterally terminate the Contract if, during the performance of the Contract, any of the grounds referred to in Article 58(4^1) of the Law on Procurement by Contracting Entities in the Field of Water, Energy, Transport and Postal Services, and/or in Council Regulation (EU) No. 833/2014, as amended, and/or Council Regulation (EC) No. 765/2006, as amended, becomes apparent.

9. ANNEXES

9.1. Each Annex to this Contract shall form an integral part thereof. Each Party shall receive one copy of each Annex to the Contract.

9.2. Annexes to the Contract:

9.2.1. Annex to the Contract SP No. 1 — “Contact Persons”;

9.2.2. Annex to the Contract SP No. 2 — “Technical Specification”.

9.2.3. Annex to the Contract SP No. 3 — “Service Fees”;

9.2.4. Annex to the Contract SP No. 4 — “Confidentiality Agreement”;

9.2.5. Annex to the Contract SP No. 5 — “Agreement on the Processing of Personal Data”.

10. DETAILS OF THE PARTIES

Service Provider	**Buyer**
MailerLite Limited Ground Floor, 71 Lower Baggot Street, Dublin 2 D02 P593, Ireland Company code: 689826 VAT code: IE3748416JH S/a No. BE44 9671 8976 9045 Bank: TransferWise Europe SA Bank code: TRWI Tel.: No.: - Fax: -	**AB Lietuvos paštas** Registered office address J. Jasinskio g. 16, LT-03500 Vilnius, Republic of Lithuania Company code 1212155811 Tel.: +370 700 55 400 E-mail: info@post.lt S/a LT71 7044 0600 0018 7388 AB SEB bankas Bank code 70440
Director	Director of the Business Development and Technology Department

CONTACT PERSONS

1.	The Buyer's representative responsible for the execution of the Contract on the Buyer's side	
2.	The Buyer's representative responsible for the publication of the Contract and amendments thereto in accordance with the law	
3.	The representative responsible for the performance of the Contract on the Supplier's side	
4.	In the absence of the responsible persons referred to in points 1 to 3, the staff replacing them shall be deemed to be responsible for carrying out the functions referred to in those points.	

TECHNICAL SPECIFICATION

1. TERMS AND ABBREVIATIONS

1.1. **Buyer / Contracting Entity — Joint Stock Company Lietuvos paštas**
1.2. **Supplier** — an economic entity — a natural person, a private or public legal person, another organisation and their subdivisions, or a group of such persons, including temporary associations of economic entities, with which the Buyer will conclude a contract for this Procurement.
1.3. **Contract** — the Purchase Contract, concluded between the Supplier and the Buyer in respect of the Object of Procurement.

2. OBJECT OF THE PROCUREMENT

2.1. The object of the procurement is the purchase of services for an email system (hereinafter — services).
2.2. The object of the procurement is not subdivided into lots, so the Supplier must submit a tender for the whole of the scope of the procurement specified below.
2.3. The start date for services is 5 working days from the date of signature of the contract.
2.4. Scope of services:

Table 1.

Ord. No.	Name of service	Exact volume of service provision, mths	Provision of services	
			Yes (tick if service requests will be made on demand, periodically, etc.)*	**No** (tick if the full quantity of services to be procured will be delivered at the time indicated)**
1.	E-mail service	12	■	☐

2.4. Orders for the upload of 4 templates, as well as for various consultancy services during the term of the Contract (as described in item 12 of Table 2), may be placed throughout the term of the Contract, according to the Buyer's need.

3. SERVICE REQUIREMENTS

Table 2

Description and requirements
1. Creating e-mails: 1.1. the content editor must operate on a drag-and-drop logic; 1.2. there shall be functionality to create content automatically by scanning from a link; 1.1. there shall be functionality to create content automatically by generating emails from JSON; 1.2. there shall be functionality to create content automatically by generating emails from RSS feeds; 1.4. HTML code upload; 1.5. uploaded content, including images, must be editable; 1.6. ability to create text e-mails.
2. Working with templates: 2.1. the supplier must provide the service of uploading the template into the system (no additional charge); 2.2. it must be possible to create and use e-mail templates; 2.3. it must be possible to create your own templates using HTML; 2.4. template upload deadlines: 2.4.1. no more than 5 working days from the date of placing the order (design material); 2.4.2. a maximum of 2 working days to review the results and submit corrections; 2.4.3. a maximum of 3 working days for corrections.
3. Recipient management: 3.1. it must be possible to:

3.1.1. create a recipient;
3.1.2. upload the recipient from XLS, TXT, CSV files (only .XLS is required, others are preferred);
3.1.3. upload and manage the recipient via an API (Application Programming Interface);
3.1.4. erase the recipient;
3.1.5. forget the recipient;
3.2. the possibility of creating groups of recipients must be realised;
3.3. the possibility of segmenting recipients must be realised;
3.4. recipient group statistics must include:
3.4.1. average number of openings;
3.4.2. average number of clicks;
3.4.3. average number of registrations;
3.4.4. average refusal rate;
3.4.5. a graph of the evolution of the number of recipients;
3.4.6. the recipients' reading interface (app, browser, or mobile device);
3.4.7. the most popular recipient domains.
3.5. the possibility for the recipient to easily unsubscribe from emails (unsubscribe function) must be implemented;
3.6. the possibility for unsubscribers to be added to the list or statistics as “not wishing to receive newsletters” must be implemented;
3.7. generation of Lithuanian forms of address (mandatory).

4. Sending:
4.1. e-mails must be able to be sent in accordance with the following:
4.1.1. set times;
4.1.2. at intervals in accordance with the quantity and timing specified;
4.2. for sending emails — the database must be able to be filtered by attributes (based on the content of the database columns);
4.3. A/B testing capability (mandatory);
4.4. repeated sequences of e-mails.

5. Statistics:
5.1. the statistics must reflect all e-mail opens regardless of the device and e-mail viewer used;
5.2. the reports must generate information both through the perspective of a single recipient and a single newsletter;
5.3. the statistics of all newsletters must be visible;
5.4. all sent newsletters must be stored with information on when the newsletter was sent and to which recipients (as well as to which segments);
5.5. mandatory reporting data:
5.5.1. reads and clicks;
5.5.2. Spam complaints, Denials, Rejections (Hard and Soft separately);
5.5.3. a graph of reads and clicks over time;
5.5.4. reading interface (app, browser, or mobile device);
5.5.5. the most popular e-mail systems;
5.5.6. link activity;
5.5.7. a general overview of the reports for the selected period.
5.6. the report must be able to show how many newsletters are sent per recipient per month.
5.7. Monthly statistics as well as the total number of all e-mails should be visible.
5.8. accessibility indicators;
5.9. e-commerce statistics.

6. Automatic e-mails:
6.1. it must be possible to prepare automated e-mails. Possible sending options:
6.1.1. an automated e-mail is sent when the recipient enters a group;
6.1.2. an automated e-mail is sent on a specific date;
6.1.3. an automated e-mail is sent when the recipient's information changes;
6.1.4. an automated e-mail is sent to the recipient after clicking on the links in the e-mails sent.
6.2. it must be possible to view/generate reports of automated e-mails.

7. Transactional e-mails:
7.1. it must be possible to prepare transactional e-mails;
7.2. transactional e-mails must have versions;
7.3. it shall be possible to view/generate reports of transactional e-mails.

8. Subscription forms:
8.1. it must be possible to create and use recipient subscription forms;
8.2. subscription forms may be embedded in the website or used separately;
8.3. subscription forms must have a registration confirmation function.

9. System user management and rights: 9.1. an unlimited number of users must be allowed; 9.2. each user of the system must be defined: 9.2.1. NT Authentication; 9.2.2. information that can be viewed by the user; 9.2.3. information that can be changed by the user. 9.3. it must be possible to define a super user who is allowed to perform all operations on the system; 9.4. it shall be possible to specify standard settings for the whole group, which shall apply if the operator has not defined any personal settings; 9.5. the system must contain audit information on data transactions. The audit trail must contain information on the actions performed on the data, the users who performed the actions on the data, the dates, the time records.
10. Reliability requirements: 10.1. the updating and modernisation of the application system must preserve the information accumulated; 10.2. the system must be capable of automatically backing up and restoring from backup all stored data.
11. System software requirements: 11.1. fast dispatch of e-mails (at least 200 e-mails in 1 s); 11.2. the system must support Unicode characters; 11.3. the system must automatically provide information messages in accordance with the rules; 11.4. the software must not have limits on the size of the database.
12. Need and other requirements: 12.1. Up to 5 million e-mails must be able to be sent to up to 0.2 million unique recipients over the lifetime of the contract. 12.2. Services will be procured based on the Buyer's actual need. 12.3. The price quoted must also include the uploading of the templates (see point 2 of this table), as well as various consultancy services for the duration of the contract. 12.4. The start of use of the system is specified in clause 2.3 (Before the start of the provision of services, a primary user (if required) must be created, and logins or other necessary information must be provided).

SERVICE FEES

Name of service	**Fee per month for the provision of services Eur excluding VAT[1]**
1	*2*
E-mail system services (including uploading of 4 templates, consultation and system set-up)	*405.30*

[1] Not applicable pursuant to Article 13(2) of the Law of the Republic of Lithuania on Value Added Tax

CONFIDENTIALITY Agreement

Joint Stock Company Lietuvos paštas, legal entity code 121215587, registered office address J. Jasinskio g. 16, Vilnius (hereinafter — the Buyer), represented by the Director of the Business Development and Technology Department, , acting in accordance with the order No. 1-2021-00001 of 4 January 2021 of the Director General of the Joint Stock Company Lietuvos paštas, and acting under the Articles of Association of the Company,

and **MailerLite Limited**, legal entity code 689826, with registered office at Ground Floor, 71 Lower Baggot Street, Dublin 2 D02 P593, Ireland, (hereinafter — the Supplier), represented by its Director,

hereinafter the Buyer and the Supplier may be collectively referred to as the "Parties" and each individually as a "Party",

it being understood that:

- the parties entered into a service contract under which the Supplier undertook to provide the Buyer with the services of an email system (hereinafter — the Service Contract);
- The Supplier's performance of the Services Contract will result in the disclosure of and/or access to data relevant to the Buyer and its business which constitutes confidential information;
- the unauthorised disclosure of such confidential information to third parties may cause damage to the Buyer and/or its business interests,

have agreed and entered into this confidentiality agreement (hereinafter — the Agreement):

1. CONCEPT OF CONFIDENTIAL INFORMATION

1.1. Confidential information:

1.1.1. any information in any form (written, oral, electronic, visual and/or other) which the Buyer communicates or discloses to the Supplier and which constitutes the Buyer's trade and/or technological secret, including commercial experience, information relating to the Buyer's commercial technologies, the Buyer's business model, know-how and/or other information, which has commercial value, the confidentiality of which the Buyer seeks to preserve, including but not limited to information relating to the Buyer's operating procedures, human, intellectual and material resources, contracts, partners, all counterparties, business projects, negotiations with partners, operational and/or business policies, customers. Confidential information includes information relating to the number of the Customer's clients, the composition of the Customer's clients, their personal data, procedures for the provision of the Services, pricing of the Services, the Customer's financial and accounting data, information systems information (schematics, drawings, technology, equipment manufacturers/models/versions, software manufacturers/models/versions, security systems, processes, any information contained in information systems/databases, source codes), the technologies, systems used in the Buyer's business, the principles of operation of the business management system, the evaluation algorithms used by the system, the performance of the Buyer's obligations to the Buyer, any data about the Buyer's customers that the Buyer has provided or otherwise made known to the Supplier, the prices offered and charged by the parties to each other, any other information relating to the Buyer and the Buyer's subsidiaries;

1.1.2. all databases, analyses, notes, explanations, other documents prepared by the Buyer or by third parties engaged by the Buyer which contain or are based on the information referred to in Clause 1.1.1 of the Agreement;

1.1.3. any materials created by the Buyer and in any form (written, electronic and/or otherwise) documents (whether in paper or electronic form) transmitted to the Supplier which are not covered by Clauses 1.1.1 and/or 1.1.2 of the Agreement;

1.1.4. information regarding the specifics of the cooperation between the Parties, as well as any correspondence between the Parties relating to cooperation under the Service Contract, this Agreement, the Service Contracts, this Contract, the terms and conditions thereof, the Annexes and/or copies thereof, and any other information communicated in connection with the performance of these agreements.

1.2. If the Supplier is in doubt as to whether certain information provided by the Buyer or otherwise coming to its attention relating to the Buyer is confidential, the Supplier shall treat such information as confidential in accordance with the procedures set out in this Agreement, unless the Buyer confirms otherwise in writing. Confidential information is not considered to be publicly available information.

2. SUBJECT MATTER OF THE AGREEMENT

2.1. The Supplier undertakes to use the information received from the Buyer only for the following purpose: for the performance of the Service Contract concluded between the parties. The Supplier also undertakes to protect confidential information, not to disclose confidential information to any third party, and to ensure that confidential information is not made available in any form to persons not entitled to receive it.

3. RIGHTS AND OBLIGATIONS OF THE SUPPLIER

3.1. The Supplier undertakes to use the confidential information received or made known to it from the Buyer only for the purpose set out in Clause 2.1 of the Agreement.

3.2. The Supplier shall be entitled to disclose confidential information or parts thereof only:
3.2.1. to those employees of the Supplier who are required to have access to confidential information to perform the Agreement;
3.2.2. with the prior written consent of the Buyer, to third parties engaged by the Supplier if they need access to confidential information to perform the Agreement;
3.2.3. to the relevant state authorities, officials, and other persons to whom such information must be disclosed in accordance with the mandatory provisions of the laws of the Republic of Lithuania (only that part of the information which is required to be disclosed at the lawful request of the aforementioned persons). In such a case, the Supplier shall immediately inform the Buyer in writing upon being requested to disclose confidential information entrusted to it by the Buyer.

3.3. The Supplier shall inform persons to whom confidential information is lawfully disclosed that the information is confidential and shall ensure that any person who will deal directly or indirectly with, have access to, and/or have access to, or access to, the confidential information complies with the terms and conditions of this Agreement, protect the confidential information, not disclose the confidential information to third parties who are not entitled to receive it and not use it for personal purposes, and undertake in writing to deal with the confidential information in the manner provided for in the Agreement, and to be jointly and severally liable with the Supplier for any breach of its obligations.

3.4. The Supplier undertakes to implement technical and organisational measures to protect the security of confidential information received or made known, so that persons not entitled to receive or know such information do not have the means and conditions to receive or know it.

3.5. The Supplier shall immediately notify the Buyer if it knows or has reasonable grounds to suspect that confidential information may be or has been disclosed to persons not entitled to receive or know it, and shall use its best endeavours to prevent and remedy such breaches and to bring the offenders to legal action or any other lawful remedy.

3.6. The Supplier shall keep the confidential information in strict confidence and shall not discuss, transmit, or otherwise disclose it to any third party, except as provided for in this Agreement, and shall not make any copies, transcripts, extracts, and/or other records of the confidential information, except as necessary for the performance of the Services Contract, keep the confidential information in a careful, safe, and secure place and not to carry it around or dispose of it in such a way that it may be lost, misplaced or otherwise come under the Supplier's control, and to take such other measures as may be necessary to prevent unauthorised reproduction, use, and/or disclosure of confidential information.

3.7. The Supplier undertakes to ensure that, neither during the term of the Service Contract nor after its termination, confidential information in any form whatsoever, and any copies thereof, shall be made available to persons not entitled to receive it.

3.8. Upon the Buyer's specific written request, the Supplier shall, within 20 (twenty) working days after the information received from the Buyer is no longer used for the purposes set out in the Agreement, destroy and/or completely erase, or shall oblige the person to whom the confidential information was disclosed to destroy or completely erase, all documents in which the confidential information is contained, without retaining any copies of the information in any medium. The Supplier shall immediately provide the Buyer with written confirmation of the fulfilment of the requirements set out in this clause of the Agreement. If requested by the Buyer, the Supplier shall, within five (5) working days, return all tangible media of confidential information in its possession to the Buyer and shall ensure that the tangible media of confidential information in its possession are returned by all other persons to whom such information has been communicated.

4. LIABILITY

4.1. If the Supplier, without the Buyer's written consent, discloses to third parties in any manner whatsoever any confidential information provided by the Buyer to the Supplier or otherwise made known to the Supplier, or otherwise breaches the Agreement, the Supplier shall pay to the Buyer a fine of EUR 3,000 (three thousand euros) for each breach of the Agreement. However, if the loss suffered by the Buyer exceeds the amount specified in this clause of the Agreement, the Supplier shall be obliged to compensate for the loss exceeding the amount specified, as well as for the loss of income by the Buyer and the loss of income derived by other persons from the unauthorised use of the Buyer's confidential information disclosed by the Supplier.

4.2. The amount referred to in Clause 4.1 of this Agreement shall be deemed to be the Buyer's predetermined future minimum loss and the Buyer shall not be required to prove the amount of its loss in such case. The Parties agree that the amount of damages agreed between the Parties is not excessive and is reasonable, taking into account the scope of the Parties' obligations and the consequences of the Supplier's failure to properly perform its obligations to the Buyer, and does not prejudice the balance of interests of the Parties.

4.3. In the event of a breach of the Agreement, the Supplier shall pay to the Buyer the amount referred to in Clause 4.1 of this Agreement within 30 (thirty) days of the date of each such breach.

5. FINAL PROVISIONS

5.1. This Agreement shall enter into force on the date of entry into force of the Service Contract and shall remain in force for a period of 5 (five) years after the expiry of the Service Contract. The Agreement shall apply and apply both to confidential information communicated and/or otherwise disclosed by the Buyer to the Supplier before the entry into force of this Agreement and to confidential information disclosed and/or otherwise communicated by the Buyer to the Supplier after the entry into force of this Agreement.

5.2. If the Parties enter into other contracts after the entry into force of this Agreement, this Agreement shall continue to apply to the relationship between the Parties arising before, during and after the term of the Agreement, unless otherwise provided for in the Agreement (as used in the text of the Agreement, the term “Service Contract” shall include any other contract between the Parties referred to in this Clause of this Preamble to the Agreement).

5.3. The provisions of the Agreement shall not apply to information that is not considered confidential.

5.4. The Agreement may be amended or supplemented by written agreement between the parties.

5.5. The Agreement shall be governed by the law of the Republic of Lithuania.

5.6. Neither party shall have the right to assign its rights and obligations under the Agreement, or any part thereof, to any third party without the written consent of the other party.

5.7. The Agreement is drawn up in the Lithuanian language in a simple written form in two copies having equal legal force. Each Party shall retain one copy of the Agreement.

5.8. Disputes between the Parties shall be settled by negotiation. In the event of failure to reach an amicable settlement, the dispute shall be settled in accordance with the laws of the Republic of Lithuania before a court located in Vilnius city.

Supplier

MailerLite Limited
Ground Floor, 71 Lower Baggot Street, Dublin 2
D02 P593, Ireland
Company code: 689826
VAT code: IE3748416JH
S/a No. BE44 9671 8976 9045
Bank: TransferWise Europe SA
Tel.: No.: -
Fax: -
E-mail: info@mailerlite.com

Director

Buyer

AB Lietuvos paštas
J. Jasinskio g. 16, 03500 Vilnius
Company code: 121215587
VAT code: LT212155811
S/a No. LT71 7044 0600 0018 7388
AB SEB bankas
Tel.: No.: 8 700 55 400
Fax: (8 5) 216 3204

Buyer's representative

Director of the Business Development and Technology Department

AGREEMENT ON THE PROCESSING OF PERSONAL DATA

Joint Stock Company Lietuvos paštas, legal entity code 121215587, registered office address J. Jasinskio g. 16, 03500 Vilnius, Lithuania, represented by the Director of the Business Development and Technology Department (**hereinafter — the Controller**) and MailerLite Limited, *legal entity code* 689826, located at Ground Floor, 71 Lower Baggot Street, Dublin 2 D02 P593, Ireland, represented by the Director (**hereinafter Manager**), have entered into the following agreement on the processing of personal data (**hereinafter — Agreement**). The Controller and the Manager are collectively referred to in the Agreement as the "Parties" and each may be referred to individually as a "Party".

The Agreement governs the processing of personal data arising out of the contract for the provision of email system *services* (**hereinafter — the Master Agreement**).

In implementing the Agreement, the Parties shall be guided by the General Data Protection Regulation (EU) 2016/679 (hereinafter — **GDPR**), the Law on Legal Protection of Personal Data of the Republic of Lithuania, and other legal acts regulating the processing of personal data (hereinafter collectively — the **Personal Data Protection Laws**).

Capitalized terms used in this Agreement shall have the meaning ascribed to them in this Agreement and/or the Master Agreement. Other terms used in the Agreement shall be understood as defined in the Personal Data Protection Legislation.

I. Basis, purpose, and scope of processing of personal data

1. The basis, purpose, and scope of the processing of personal data by the Manager are set out in this Agreement.
2. Personal data is processed based on the performance of the Master Agreement to ensure the proper performance of the Manager's obligations under the Master Agreement and compliance with the requirements of the Personal Data Protection Legislation.
3. The Parties agree that this Agreement constitutes a documented processing instruction from the Controller. The Parties agree that during the term of the Agreement and in the case of processing of personal data after its termination, the Controller may provide additional instructions. If the Manager does not have instructions on how to process personal data in a particular situation, or if, in the opinion of the Manager, the instructions provided by the Controller are in breach of the legislation on the protection of personal data, or are unclear, the Manager shall inform the Controller in writing without delay.

II. Instructions from the Controller regarding the processing of personal data and the Manager's obligations

General obligations of the Controller regarding the processing of personal data

4. The Controller undertakes to process personal data in accordance with the Personal Data Protection Legislation, the Agreement and the Manager's documented instructions, including about the transfer of personal data to a third country or an international organisation unless required to do so by the law of the European Union or of a Member State to which it is subject. In such a case, the Manager shall inform the Controller in writing of such legal requirement before processing the personal data, unless such notification is prohibited by that law for imperative reasons of public interest.
5. The Manager shall ensure that its employees or other persons lawfully authorised to process personal data:
5.1. are duly informed of the confidentiality of personal data;
5.2. are properly trained in the processing of personal data;
5.3. are committed to ensuring the confidentiality of the personal data processed during the processing period and indefinitely thereafter;
5.4. will only process personal data where this is necessary for the performance of their direct functions.
6. The Manager undertakes to ensure the security of the personal data processed at its own expense by implementing appropriate technical and organisational measures, which shall be chosen, inter alia, in accordance with the requirements laid down in Article 32 of the GDPR. The Manager also undertakes to implement the Security Requirements set out in Annex 1. The Manager undertakes to implement the technical and organisational measures and the Security Requirements referred to in this point before the beginning of the processing of personal data and to apply them throughout the entire period of processing of the personal data, to monitor, control and, if necessary, update them.
7. The Manager shall assist the Controller promptly to ensure compliance with the obligations set out in Articles 32 to 36 of the GDPR, taking into account the nature of the processing of the personal data and the information available to the Manager.

8. Upon the Controller's request, the Manager undertakes to provide the Controller with information, within a reasonable period of time specified by the Controller, on the Manager's compliance with the requirements set out in the Agreement, the Controller's other documented instructions, and the Personal Data Protection Legislation.
9. The Manager shall indicate in the section of this Agreement entitled "Terms and Conditions of Processing of Personal Data" whether it, and the sub-processor, if any, engaged by it, process personal data within or outside the European Economic Area. If, during the period of processing of personal data, the Manager or its sub-processor, if any, plans to process personal data outside the European Economic Area, the Manager must inform the Controller 30 (thirty) calendar days in advance, provide all the information requested by the Controller, obtain the Controller's prior consent to such processing of the personal data, and, where necessary, sign additional agreements for such processing of personal data (e.g., standard contractual clauses as defined in a decision of the European Commission).
10. The Manager undertakes to keep records relating to all categories of personal data processing activities carried out on behalf of the Manager in accordance with the requirements of Article 30(2) of GDPR.
11. In addition to the obligations set out in this Agreement, the Manager must comply with other obligations set out in the Personal Data Protection Legislation.

Data breach

12. In the event of a data breach or where the Manager has reason to believe that a data breach has occurred, or in the event of any action by the State Data Protection Inspectorate against the Manager in relation to personal data processed under this Agreement, the Manager shall immediately notify the Controller in writing, free of charge, at the contact details provided for in the Master Agreement and by email, no later than 48 (forty-eight) hours from the time of the aforesaid actions, without charge, at the contact details provided for in the Master Agreement and by e-mail duomenusauga@post.lt. The Manager shall take measures to prevent further damage, to mitigate the effects of the data breach without delay and charge, and to inform the Controller of the investigation of the data breach and the related actions.
13. Together with the notification provided for in paragraph 12, the Manager shall provide the Controller with a notification containing all the information that is necessary for the Controller, in accordance with the Personal Data Protection Legislation, to be able to fulfil its obligation to notify the State Data Protection Inspectorate and/or data subjects of a data breach and to remedy and/or mitigate the consequences of the data breach in a timely and appropriate way. In the event of a request for additional information from the Controller, the Manager shall promptly provide such information free of charge within a time limit specified by the Controller.
14. The Manager must take all necessary measures and actions following a data breach to prevent the occurrence of such or similar data breaches in the future.
15. The Manager shall document any breaches of security of personal data processed under the Agreement and the Master Agreement, including the facts relating to the breach, the consequences of the breach, and the corrective action taken.

Enforcement of data subjects' rights and related actions

16. If the Data Subject, a supervisory authority or a third party, in accordance with the Personal Data Protection Legislation and/or other legislation, requests the Manager to provide any information about the personal data processed under this Agreement, including the exercise of the rights of the Data Subjects, the Manager shall promptly, but no later than within 3 (three) days, forward such request to the Controller.
17. The Manager undertakes not to provide the response to the data subject, supervisory authority or third party who has made the request referred to in point 16 without the Controller's prior written authorisation to do so, unless the Manager is obliged by law to provide such information. In this case, the Manager shall inform the Controller in advance, at least three (3) working days in advance, by providing the legal basis for the provision of the information, the recipient of the information, the content of the information, the planned date of its provision, as well as other information requested by the Controller.
18. Irrespective of whether the request for information, including the exercise of the rights of data subjects, as provided for in point 16 has been received by the Manager or by the Controller, the Manager undertakes to assist the Controller in the preparation of a response and, if necessary, to comply with the relevant requirements, free of charge, promptly and to the extent necessary.

Right to audit, including inspections

19. The Manager undertakes to facilitate and assist the Controller's right to carry out audits and inspections of the Controller, free of charge, insofar as it relates to personal data processed under the Agreement.
20. The Controller shall have the right to carry out audits and inspections of the Manager, free of charge, at the premises of the Manager's head office or other premises where personal data processing operations are carried out, during normal working hours, upon prior notice, without interrupting the Manager's activities. Such audits, inspections may be carried out by employees of the Controller or by other persons authorised by the Controller and bound by appropriate confidentiality obligations.
21. The Controller undertakes to keep the results of audits and inspections confidential and to use them only to the extent necessary to ensure the proper processing and security of personal data processed under this Agreement.

22. The Controller shall have the right to propose to the Manager an audit, inspection, or verification of the sub-processor it has engaged. If the Manager refuses to carry out an audit or inspection upon receipt of such a proposal, such refusal shall be clearly and reasonably substantiated.
23. The costs of audits and inspections shall be borne by the Party initiating them. If audits or inspections reveal non-compliance or improper compliance with this Agreement or Personal Data Protection Laws by the Manager, its employee, its authorised or otherwise related persons, the sub-processor, the Manager shall be obliged to bear the costs of the Controller's audits or inspections and to remedy the identified breaches promptly and at the Manager's own cost.

Sub-organisation of personal data

24. The Controller does not provide general written prior approval for the use of sub-processor(s), i.e., the Manager may only use a sub-processor after having informed the Controller in writing in advance (within an objectively reasonable period of time) and having obtained its prior written approval.
25. If the Manager has already engaged sub-processor(s) before entering into this Agreement, the Manager shall inform the Controller before entering into this Agreement and provide information about the sub-processor(s) in the section of this Agreement entitled “Terms and Conditions for Processing Personal Data”.
26. Before transferring the processing of personal data to a sub-processor, the Manager must check and make sure that the sub-processor is adequately equipped to ensure compliance with the requirements set out in this Agreement, in other instructions of the Controller, and the legislation on the protection of personal data. The Manager shall document such verification and, if requested by the Controller, make it available within a time limit set by the Controller. The requirements set out in this clause shall also apply if the contract between the Manager and the sub-processor was concluded before this Agreement.
27. The Manager undertakes to subject its sub-processor(s) to the same obligations for the protection of personal data as it is subject to under this Agreement and the Personal Data Protection Legislation applicable to it. The requirements set out in this clause shall also apply if the contract between the Manager and the sub-processor was concluded before this Agreement.
28. Upon the request of the Controller, the Manager undertakes to provide, within a time limit specified by the Controller, the main terms and conditions of the contract concluded with the sub-processor, including those relating to the protection of personal data, and to answer the Controller's questions relating to the sub-processing of personal data.
29. If the Controller objects to the use of a new sub-processor or to further sub-processing by an existing sub-processor, the Manager must continue to comply with its obligations under the Master Agreement, the Agreement, other instructions from the Controller and the Personal Data Protection Laws.
30. The Manager shall inform the Controller in advance, but no later than ten (10) working days before terminating the contract with the sub-processor and shall provide information on how the termination of the contract will affect the fulfilment of the Manager's obligations provided for in the Agreement, in the Controller's other instructions, and the legislation on the protection of personal data.

Actions following processing of personal data

31. Upon termination of the Agreement and deletion of the email account by the Controller, the Manager shall, within 30 (thirty) calendar days, irretrievably and irreversibly delete the personal data contained in the Controller's system, copies thereof (and in the case where the data, copies thereof, are processed in paper format, securely destroy them), except in cases where the retention of personal data is required by the legislation of the European Union or a Member State. In such case, the Manager shall inform the Controller of such legal requirements before the signing of this Agreement and shall become fully and exclusively responsible for such legally required processing of such personal data. The Manager shall inform the Controller of the erasure of the data provided for in this point within the time limit provided for in this point.
32. The Manager shall ensure that the sub-processor(s) it has engaged at the end of this Agreement comply with the requirements set out in point 31.

III. Liability

33. The Manager shall indemnify all costs, expenses, fines, damages and losses caused to personal data subjects, the Controller, the Controller's employees, the Controller's clients, cooperation partners or third parties by the Controller, its employees, authorised persons, sub-processor(s) in the course of improper performance in breach of the Agreement, other instructions of the Controller, the Personal Data Protection Laws and any other legal regulations. The Parties agree that any limitations of liability contained in the Master Agreement or other agreements between the Parties shall not apply to this Agreement.

IV. Final Provisions

34. Annex 1 is an integral part of this Agreement and shall be interpreted in accordance with the provisions of the Agreement.
35. Any breach by the Manager, its employees, authorised persons, sub-processors of the obligations set out in the Agreement, other instructions of the Controller, Personal Data Protection Legislation may be considered a material breach

of the Agreement and/or the Master Agreement and the Controller may terminate the Master Agreement, including this Agreement, in accordance with the procedures and terms set out in the Master Agreement.

36. The Manager shall not be entitled to any compensation for costs incurred in complying with its obligations under the Agreement, other instructions of the Controller, Personal Data Protection Laws.

37. The Agreement shall enter into force on the date of its signature and shall remain in force until the deletion of the personal data processed under it.

38. The legal relationship between the Parties under this Agreement shall be governed by the Personal Data Protection Legislation, which shall include the law of the Controller's home country, i.e., the laws and regulations of the Republic of Lithuania, as well as the directly applicable legislation of the European Union.

39. The Agreement is an integral part of the Master Agreement. In the event of any conflict between this Agreement and the Master Agreement in the area of personal data protection, the provisions of this Agreement shall apply.

40. This Agreement shall be subject to all the general provisions of the Master Agreement except those specifically addressed in this Agreement.

V. Terms and Conditions of Processing of Personal Data

Completed by the Controller:

Categories of data subjects	Employees of the Controller, Clients of the Controller
Types of data processed	Employees of the Controller: the e-mail address for logging into the Manager's system. Customers of the Controller: full name, e-mail address (some or all of the following data may be transmitted)
Processing operations to be carried out	Entering personal data into the Manager's system, sorting it, categorising it into groups, and sending newsletters to specific groups.
Methods of data provision (how the Controller transfers data to the Manager)	The .csy file is uploaded to the Manager's system.

Completed by the Manager:

Places where the Manager stores personal data (specific country within or outside the European Economic Area)	
Contact details (e-mail address and telephone number) of the Data Protection Officer of the Manager	

Information on the sub-processor

(if the Manager uses more than one sub-processor, the table contains information on each of them).

Where information on the sub-processor is already provided during the performance of the Agreement, it may be provided in a manner agreed by the Parties (e.g., as an annex to the Agreement, as a letter from one Party to the other Party).

Name, legal entity code, registered office address/full name, date of birth or individual activity number, residential address	**Google Ireland Limited**, Legal entity code 368047, Registered address Google Building Gordon House, Barrow St, Dublin 4, Ireland
Processing of personal data by the sub-processor	Data centre in [illegible]
Personal data transferred to the sub-processor for processing	All personal data provided by the Controller
Date, number, name, and term of the contract with the sub-processor	23-06-2021, Indefinite
Location where the sub-processor holds the personal data (specific country within or outside the European Economic Area)	

VI. Details and signatures of the Parties:

CONTROLLER:	**MANAGER:**
Joint Stock Company Lietuvos paštas Legal entity code 121215587 J. Jasinskio g. 16, 03500 Vilnius	MailerLite Limited
Director of the Business Development and Technology Department	Director

Annex No. 1 to the Agreement

Security requirements

The Manager, its employees, as well as the sub-processor(s) employed by the Manager, shall comply with the recommendations or other legal documents adopted by the supervisory authority on the application of technical and organisational data security requirements, as well as the minimum technical and organisational security requirements set out in this Annex.

I. Computing, software, cloud services

1. Computerised workstations, which include, but are not limited to, an employee's personal computers, mobile phones and other similar equipment used for work purposes, both on the Manager's premises and when the Manager's employees are working remotely (hereafter — **CWSs**) and on servers:

1.1. only computer hardware and software supported by the manufacturers must be used;

1.2. patches to fix critical and important security vulnerabilities in software must be in place;

1.3. separate accounts must be used for routine work and the administration of the CWS;

1.4. a password of at least 8 characters, using 3-character groups (lower case, upper case, and numbers), must be used to log on to the CWS and other objects on the computer network (servers, firewalls, and other equipment connected to the network) and must be changed regularly;

1.5. real-time anti-virus software must be used (must be up and active at system startup); the virus database must be updated before scanning and must automatically scan files before they are opened or started;

1.6. a firewall shall be used that only misses returning data packets from device-initiated sessions and only data packets from sessions described by exceptions, and shall not send a response to the sender of a data packet after blocking an unauthorised packet;

1.7. the internal data drives of portable CWSs shall be fully encrypted;

1.8. system event records shall be generated, processed, and stored, structured as follows: event type; user identifier; date and time; record of successful and unsuccessful access; system components or resources involved; IP address of the network and/or protocol used;

1.9. a malware protection system must be in place to ensure that any software used to provide services to the Controller is protected against malware;

1.10. personal data must be copied and tested to ensure that the personal data are reproduced;

1.11. vulnerabilities in all relevant technologies, including but not limited to the operating system, database, applications, must be proactively and timely managed.

2. Cloud services:

2.1. the data centres must be located in a country of the European Economic Area. If, during the period of processing of personal data, the Manager or a sub-processor engaged by the Manager plans to use data centres outside the European Economic Area, the Manager shall inform the Controller by the procedure and within the time limit set out in point 9 of the Agreement;

2.3. data centre services must be certified to ISO 27001 or equivalent.

II. Selection and application of organisational and technical measures, and physical security measures

3. Taking into account the state of the development of technical capabilities, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons posed by the processing, the Manager shall put in place appropriate technical and organisational measures to ensure a level of security commensurate with the risks, including, *inter alia*, where necessary:

3.1. pseudonymisation and encryption of personal data;

3.2. the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of data processing systems and services;

3.3. the ability to restore conditions and access to personal data promptly in the event of a physical or technical incident;

3.4. a regular process of checking, evaluating, and assessing the effectiveness of the technical and organisational measures to ensure the security of processing.

4. The determination of the appropriate level of security shall take into account, in particular, the risks arising from the processing of the data, in particular the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, data transmitted, stored, or otherwise processed.

5. The Manager and the sub-processor(s) appointed by the Manager must have in place appropriate technical and organisational measures for the return of the personal data to the Controller and/or their erasure after the end of the processing period, as well as appropriate technical and organisational measures for the exercise of the rights of the data subjects.

6. The Manager shall ensure that personal data processed under this Agreement are processed separately from other personal data of the Manager, including but not limited to personal data under the Manager's own control.

7. Taking into account the criteria set out in point 3, the Manager shall select and apply different physical security measures for different data processing locations (e.g., office premises, data centres, server rooms).

III. Access granting, operational security, and related requirements

8. The Manager shall establish a list of employees or other legally authorised persons to whom it grants access to the Controller's personal data and shall review and, if necessary, update it regularly, at least once every 3 months. The Manager shall ensure that such persons' access is properly managed and that access is granted and/or revoked promptly.
9. The Manager's access to the Controller's personal data must be personalised, i.e., linked to a specific employee of the Manager. The Manager, its employees shall not grant access (i.e., new access, extension of existing access, renewal of access, extension of access, etc., or in any other way provide access to the network, etc.) to any other person without the prior written consent of the Controller.
10. The Manager shall use secure (2-factor) authentication for systems containing the Controller's data for system administrators or other highly privileged users, including remote access users.
11. The Manager shall ensure that each of its employees has a personal and unique identifier (user ID) and shall use an authentication method that confirms and ensures the identity of users.
12. The Manager must have a change management system in place for changes to business processes, information handling facilities, and systems. The change management system must include tests and reviews before changes are implemented, such as procedures for handling urgent changes, procedures for recovering from failed changes, and records that show what was changed, when it was changed, and by whom.
13. The Manager shall record and monitor the activities of users, including system administrators, successful and unsuccessful logins, data processing operations performed, exceptions used, failures, and information security events, and shall review them regularly. In addition, the Manager shall keep and retain the recorded information for a minimum period of 6 months, or such longer period as may be required by law, and shall make it available to the Controller upon request.
14. The Manager must actively and timely manage vulnerabilities in all relevant technologies, including but not limited to the operating system, database, application.
15. The Manager shall establish security requirements for all relevant technologies such as operating systems, databases, applications.
16. The Manager must ensure that development is separated from the testing and production environment.

IV. Managing security incidents, including data breaches, and business continuity

17. The Manager shall have procedures in place to manage security incidents, including data breaches.
18. The Manager shall promptly provide the Controller with a duly compiled and accurate security incident report and shall comply with its other obligations relating to data breaches under the Agreement.
19. The Manager shall identify the risks to business continuity and take the necessary steps to control and mitigate those risks.
20. The Manager shall document its business continuity management processes and procedures.
21. The Manager shall periodically assess the effectiveness and compliance of its business continuity management.
22. The Manager shall provide reports on the proper functioning of the business continuity measures at the request of the Controller.

V. Security Compliance

20. At the request of the Controller, the Manager shall promptly provide the Controller with a report on compliance with the Security Requirements, which shall include the compliance of the sub-processor(s), if any, with these requirements.

VII. Details and signatures of the Parties:

CONTROLLER:	**MANAGER:**
Joint Stock Company Lietuvos paštas Legal entity code 121215587 J. Jasinskio g. 16, 03500 Vilnius	MailerLite Limited
Director of the Business Development and Technology Department	Director