# DATA PROCESSING AGREEMENT

This data processing agreement (“DPA”) is entered into by and between the Customer and SaleSqueze (as defined in the Master Software and Services Agreement and/or in the Order (the “Main Agreement”) entered into by the Customer and SaleSqueze both as identified in signature blocks of the Main Agreement (each a “Party” and collectively, the “Parties”) as of the date (i) the last Party signs this DPA or (ii) the effective date of the Main Agreement or relevant Order (“Effective Date”). In addition to the foregoing, by entering into the Main Agreement or by and as a condition to using the Platform and the Services, Customer agrees to be bound by this DPA. Under this DPA, the Customer shall be the controller and SaleSqueze the processor. Any reference to a “controller” hereunder shall be a reference to the Customer and any reference to a “processor” shall be a reference to SaleSqueze. Terms with capital letter will have the meaning ascribed to them under this DPA and under the Main Agreement.

## GENERAL

### 1. Purpose and scope

The purpose of this DPA is to ensure compliance with the Applicable Data Protection Legislation. “Applicable Data Protection Legislation" means any and all applicable data protection and privacy laws including, where applicable, Regulation (EU) 2016/679 regarding the Personal Data Protection (“GDPR”), any other applicable law which governs the agreements between the Parties in the field of data protection.

a) The controllers and processors listed in Annex I have agreed to this DPA in order to ensure compliance with the Applicable Data Protection Legislation.

b) The DPA apply to the processing of personal data as specified in Annex II.

c) Annexes I to IV are an integral part of the DPA.

d) This DPA of without prejudice to obligations to which the controller is subject by virtue of the Applicable Data Protection Legislation.

### 2. Interpretation

a) Where this DPA uses the terms defined in the Applicable Data Protection Legislation, those terms shall have the same meaning as thereinunder.

b) This DPA shall be read and interpreted in the light of the provisions of the Applicable Data Protection Legislation. This DPA is subject to and an integral part of the Main Agreement.

### 3. Docking clause

a) Any entity that is not a Party to this DPA may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to this DPA and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

## OBLIGATIONS OF THE PARTIES

**Description of processing(s)** The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

**4. Instructions**

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by the Applicable Data Protection Legislation law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor shall as soon as possible inform the controller if, in the processor's opinion, instructions given by the controller infringe the Applicable Data Protection Legislation.

**5. Purpose limitation**

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

**6. Duration of the processing of personal data**

Processing by the processor shall only take place for the duration specified in Annex II.

**7. Security of processing**

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

**8. Sensitive data**

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

**9. Documentation and compliance**

a) The Parties shall be able to demonstrate compliance with this DPA.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with this DPA.

c) The processor shall make available to the controller reasonable information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from the Applicable Data Protection Legislation, subject to confidentiality obligations. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by this DPA, if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor. The costs incurred by the processor in relation with the audit will be covered by the controller.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice and be subject to confidentiality obligations. The costs resulting from the foregoing will be paid by the controller.

e) The Parties shall make the information referred to in this DPA, including the results of any audits, available to the competent supervisory authority/ies on request.

**10. Use of sub-processors**

a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list provided in the Annexes hereunder as amended from time to time in accordance with this Clause 7.7(a). The processor shall inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 15 business days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object. If processor does not receive a written notice of objection and termination in accordance with this section, it will be deemed in good faith that the controller has accepted the change in sub-processors. If the Customer does not agree with any new sub-processor, it has the sole right to immediately terminate the Main Agreement and the DPA.

b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the similar data protection obligations as the ones imposed on the data processor in accordance with these Clauses.

c) The processor shall remain responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

**11. International transfers**

a) When the GDPR applies, any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions

from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of the GDPR.

b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, the processor and the sub-processor can ensure compliance with Chapter V of the GDPR and are hereby authorized to transfer the controller's personal data to third-countries by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of the GDPR provided the conditions for the use of those standard contractual clauses are met, or adequacy decisions.

**12. Assistance to the controller**

a) The processor shall promptly notify the controller of any request it has received from the data subject.

b) At controller's cost, the processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing.

c) In addition to the processor's obligation to assist the controller pursuant to Clause 8 (b), the processor shall assist the controller in ensuring compliance with the following obligations the other obligations for which the Applicable Data Protection Legislation provide for processor's contribution and assistance.

d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

**13. Notification of personal data breach**

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under the Applicable Data Protection Legislation, taking into account the nature of processing and the information available to the processor.

**14. Data breach concerning data processed by the controller**

In the event of a personal data breach concerning data processed by the controller and the processor, the processor shall reasonably assist the controller, if the following are under processor's control or knowledge:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to the Applicable Data Protection Legislation, shall be stated in the controller's notification

c) in complying, pursuant to the Applicable Data Protection Legislation and when expressly provided thereunder, with the obligation to communicate without undue delay the personal

data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

**15. Data breach concerning data processed by the processor**

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach;

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under the Applicable Data Protection Legislation.

## FINAL PROVISIONS

**16. Non-compliance with the Clauses and termination**

a) Without prejudice to any provisions of the Applicable Data Protection Legislation, in the event that the processor is in breach of its obligations under this DPA, the controller may instruct the processor to suspend the processing of personal data until the latter complies with this DPA.

b) This DPA is effective as of the Effective Date and will continue for the entire duration of the Main Agreement, and as long as the processor continues to process Personal Data for the Customer.

c) This DPA may be terminated by the either Party upon written notice with immediate effect, in case of the other Party's material breach of the DPA and/or for legitimate cause. This Agreement will terminate immediately upon termination of the Main Agreement. Customer understands and accepts that upon termination of this DPA, the Platform functionalities may be impacted.

d) Unless otherwise agreed between the Parties in, or in accordance with, the Main Agreement, termination of this DPA will not cause the immediate termination of the Main Agreement.

e) Following termination of the DPA, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all existing personal data to the controller and delete existing copies unless the Applicable Data Protection Legislation requires storage of the personal data.

## ANNEX I: LIST OF PARTIES

| CONTROLLER | |
|---|---|
| **Customer:** | as defined in the Main Agreement |
| **Contact person's name:** | the controller's contact is identified in the Main Agreement |

| SALESQUEZE | |
|---|---|
| **SaleSqueze:** | as defined in the Main Agreement |
| **Contact person's name:** | the controller's contact is identified in the Main Agreement as the person signing it |

## ANNEX II: DESCRIPTION OF THE PROCESSING

| Processor shall process the personal data received from the controller in accordance with the details below: | |
|---|---|
| **Categories of data subjects whose personal data is processed** | Individuals whose personal data is provided by the controller to the processor by using the Platform and the Services under the Main Agreement or for the performance of the Main Agreement, and the categories of the data subject(s) whose personal data the controller decides to be processed through the Platform and the Services, including without limitation Customer's (potential) clients, partners, employees, agents, etc. |
| **Categories of personal data processed** | The Controller determines the categories of data for the Platform and the Services used under the Main Agreement. |
| **Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.** | The Controller determines the categories of sensitive data for the Platform and the Services used under the Main Agreement. |
| **Nature of the processing** | Includes, without limitation: storage, computer processing and/or deletion, as required for the execution of controller's instructions in accordance with the Main Agreement, including, |

| | |
|---|---|
| | without limitation for the purposes of providing professional services, support, back-up, restoration, security and monitoring. |
| **Purpose(s) for which the personal data is processed on behalf of the controller** | Performing the Main Agreement concluded between the Parties and the provisions and use of the Platform and the Services.<br><br>The controller personal data will also be processed in order to send (electronic) communications to the users, according with the Platform' and the Services' functionalities and features. |
| **Duration of the processing** | For the duration of the Main Agreement, or longer when and if required by the applicable law. |
| **For processing by (sub-)processors, also specify subject matter, nature and duration of the processing.** | Provided in Annex IV. |

## ANNEX III: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

| **1. Technical and organisational measures implemented by the processor** |
|---|
| Processor has implemented an IT security policy that addresses:<br><br>• Data integrity and confidentiality;<br>• Security of IT equipment;<br>• Protection against viruses, trojans, malware;<br>• Security measures regarding databases;<br>• Back-up of data, recovery measures, provisions for periodic testing of back-ups;<br>• Security monitoring;<br>• Security incident management;<br>• Physical security;<br>• Disaster recovery;<br>• Business Continuity. |
| Processor has implemented firewall technologies to limit security risks. |
| Processor does not use production data in test, development, as well as pre-production environments. |
| Processor ensures the secure transmission of personal data inside or outside the internal network using encryption technologies so that it is not intelligible. |

| |
|---|
| Processor has installed antivirus programs and intrusion detection systems on computer systems that are updated regularly. |
| Processor reviews software and hardware used to detect and resolve vulnerabilities and defects. |
| Processor ensures that only those employees who need to carry out a processing of personal data are authorized to do so. The authorization for access to the information systems containing personal data will be granted according to the principles of "need to know" and "minimum privileges". |
| Processor through its user access policy ensures that only identified and logged-in authorized users can access the systems that manage personal data. Each authorized user has only one username. |
| Processor continuously reviews the access rights of authorized users to personal data and system components containing personal data. Access rights will be deactivated if they are not used for at least six months, except for those that have been authorized exclusively for management and technical support. Access rights will also be disabled if the authorized user is disqualified or dis-authorized to access computer systems or to process personal data. |
| Processor has established through the IT security explicit requirements for strong passwords. |
| Processor monitors access to production environments containing personal data to record the link between access and individual user and access to personal data. |
| Processor ensures the secure destruction of personal data through secure erasure procedures to make all personal data unrecoverable. |
| Processor ensures the training and education of authorized users regarding the correct rules of conduct to be adopted for the protection of personal data. |

| **2. Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller:** |
|---|
| Processor has implemented the technical and organisational measures described in *Section 1. Technical and organisational measures implemented by the processor*, of this Annex III. |

| **3. For transfers to (sub-)processors, also describe the specific technical and organisational measures to be taken by the (sub-)processor to be able to provide assistance to the controller:** |
|---|
| Sub-processors are required, whenever possible and negotiable, under the applicable data processing agreements with processor to implement adequate technical and organisational measures to be able to provide assistance to the controller. |

**ANNEX IV: LIST OF SUB-PROCESSORS**

Processor uses sub-processors to provide its products and to perform the relevant business operations under the Main Agreement. Sub-processors engaged by SaleSqueze to provide services are made available or identified upon Customer's request or in the relevant SOW for professional services. The following list of sub-processors is mandatory for SaleSqueze to operate its Services and Platform:

| Sub-processor | Purpose | Storage location | Duration of processing |
|---|---|---|---|
| **Amazon Web Services EMEA SARL** | Providing hosting, virtual infrastructure, database platform services | depending on account provisioning location | As required under the Main Agreement, unless otherwise required by the law or by sub-processor's binding rules |
| **MongoDB Limited** | Providing database platform services | Frakfurt, Europe | As required under the Main Agreement, unless otherwise required by the law or by sub-processor's binding rules |
| **MailerSend, Inc.** | Providing emailing service for transactional emails in platform | | As required under the Main Agreement, unless otherwise required by the law or by sub-processor's binding rules |
| **Microsoft Ireland Operations Ltd** | Providing integration services | depending on account provisioning location | As required under the Main Agreement, unless otherwise required by the law or by sub-processor's binding rules |
| **Sentry** | Providing log and error monitoring services | | As required under the Main Agreement, unless otherwise required by the law or by sub-processor's binding rules |
| **Post Hog** | Product usage analytics | | As required under the Main Agreement, unless otherwise required by the law or by sub-processor's binding rules |