Please fill in the highlighted blanks on pages 1 and 9, then sign the document and return it to support@resmio.com.

Annex to the "Temporary Software License" Contract –

Agreement on the Processing of Personal Data pursuant to Article 28 of the GDPR

Between

_____

(Name / Company)

_____

(Address)

- Client -

and

resmio GmbH
Katzwanger Str. 150
Building 1c
90461 Nuremberg

- Contractor –

on data processing within the meaning of Article 28 (3) of the General Data Protection Regulation ("GDPR").

PREAMBLE

This Annex specifies the obligations of the contracting parties regarding data protection resulting from the data processing ("DPA") described in detail in the Temporary Software License Contract. It applies to any and all activities which are connected to the Contract and in which employees of the Contractor or persons commissioned by the Contractor process personal data ("**Data**") of the Client.

1. Subject matter, duration and specification of the data processing

The subject matter and duration of the processing as well as the nature and purpose of the processing result from the Contract. In particular, the following data are part of the data processing:

- Personal master data (of users)
- Communication data (e.g. descriptions, comments and attachments)
- Contract master data
- Contract billing data (billing address)
- Payment data (if collected, masked)

The term of this Annex is based on the term of the Contract, unless obligations beyond this arise from the provisions of this Annex.

2. Scope of application, responsibility and place of data processing

2.1 The Contractor processes personal data on behalf of the Client. This includes activities that are specified in the Contract and in the service description. Within the scope of this Contract, the Client is solely responsible for compliance with the statutory data protection provisions, in particular for the lawfulness of data transfer to the Contractor as well as for the lawfulness of the data processing ("**Controller**" as defined in Art. 4 (7) of the GDPR).

2.2 The instructions are initially specified by the Contract and may thereafter be amended, supplemented or replaced by the Client in writing or in an electronic format

(“**text form**”) to the body designated by the Contractor by means of individual instructions (“**individual instructions**”). Instructions not provided for in the Contract are treated as a request for a change in performance. Verbal instructions have to be confirmed immediately in writing or in text form.

2.3 The contractually-agreed data processing services are exclusively provided in a member state of the European Union, or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the Client and may be effected only if the special requirements of Art. 44 et seqq. of the EU GDPR have been met.

3. Obligations of the Contractor

3.1 The Contractor may only process data of data subjects within the scope of the order for processing and the Client's instructions, unless there is an exceptional case within the meaning of Article 28 (3) a) of the GDPR. The Contractor informs the Client without undue delay if it is of the opinion that an instruction violates applicable laws. The Contractor is entitled to suspend implementation of the respective instruction until it is confirmed or changed by the Client.

3.2 The Contractor designs the internal organization within its area of responsibility in such a way that it meets the special requirements of data protection. The Contractor takes technical and organizational measures for the adequate protection of the Client's data that meet the requirements of the General Data Protection Regulation (Art. 32 of the GDPR). The Contractor takes technical and organizational measures to ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing on a permanent basis. The Client is aware of these technical and organizational measures and is responsible for ensuring that they provide an adequate level of protection for the risks associated with the data to be processed.

3.3 The Contractor supports the Client, to the extent agreed, within the scope of its possibilities in fulfilling the requests and claims of data subjects pursuant to Chapter III of the GDPR and in complying with the obligations set forth in Artt. 33 to 36 of the GDPR.

3.4 The Contractor warrants that the employees involved in the processing of the Client's data and other persons working for the Contractor are prohibited from processing the data outside the scope of the instruction. Furthermore, the Contractor warrants that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate legal duty of confidentiality. The confidentiality/non-disclosure obligation continues to exist after termination of the order for data processing.

3.5 The Contractor informs the Client without undue delay if it becomes aware of any violations of the protection of the Client's personal data.

The Contractor takes the necessary measures to secure the data and to mitigate any possible adverse consequences for the data subjects and consults with the Client on this without undue delay.

3.6 The Contractor ensures to comply with its obligations under Article 32 (1) d) of the GDPR to implement a procedure to regularly review the effectiveness of the technical and organizational measures to ensure the security of the processing.

3.7 The Contractor rectifies or erases the contractual data if the Client instructs it to do so and this is covered by the scope of instructions. If erasure in conformity with data protection or a corresponding restriction of data processing is not possible, the Contractor undertakes the destruction of data storage media and other materials in conformity with data protection on the basis of an individual order by the Client or returns these data storage media to the Client, unless already agreed in the Contract.

In special cases to be determined by the Client, storage or transfer takes place; remuneration and protective measures for this are to be agreed separately, unless already agreed in the Contract.

3.8 Data, data storage media as well as all other materials are to be either surrendered or erased at the request of the Client after the end of the order for data processing.

3.9 In the event of a claim against the Client by a data subject with regard to any claims pursuant to Art. 82 of the GDPR, the Contractor undertakes to support the Client in defending the claim to the extent of its possibilities.

4. Obligations of the Contractor

4.1 The Client informs the Contractor immediately and in full if it discovers errors or irregularities in the results of the data processing with regard to data protection provisions.

4.2 In the event of a claim against the Client by a data subject with regard to any claims pursuant to Art. 82 of the GDPR, Section 3.9 applies accordingly.

4.3 The Client informs the Contractor of the contact person for data protection issues arising within the scope of the Contract.

5. Requests by data subjects

5.1 If a data subject approaches the Contractor with requests for rectification, erasure or access, the Contractor refers the data subject to the Client, provided that an assignment to the Client is possible according to the data provided by the data subject. The Contractor immediately forwards the request of the data subject to the Client. Upon instruction, the Contractor supports the Client within the scope of its possibilities to the extent agreed. The Contractor is not liable if the request of the data subject is not answered, is not answered correctly or is not answered in a timely manner by the Client.

5.2 On the Client's documented instruction, the Contractor must directly ensure the erasure concept, the right to be forgotten, right to rectification, data portability and access, provided these are included under the scope of services.

6. Means of proof

6.1 The Contractor provides the Client with proof of compliance with the obligations laid down in this Contract by suitable means.

6.2 If, in individual cases, inspections by the Client or an auditor mandated by the Client are necessary, these inspections are carried out during normal business hours without disrupting operations after notification and taking into account a reasonable lead time. The Contractor may make such inspections dependent on prior notification with a reasonable lead time and on the signing of a confidentiality agreement with regard to the data of other customers and the technical and organizational measures that have been set up. If the auditor mandated by the Client is in a competitive

relationship with the Contractor, the Contractor has a right of objection against the auditor.

6.3 The Contractor may demand remuneration for assistance in carrying out an inspection if this is agreed in the Contract. The expenditure of an inspection is generally limited to one day per calendar year for the Contractor.

6.4 Should a data protection supervisory authority or another sovereign supervisory authority of the Client carry out an inspection, Section 6.2 applies accordingly. It is not necessary to sign a confidentiality agreement if this supervisory authority is subject to professional or statutory confidentiality where a violation is punishable under the German Criminal Code (Strafgesetzbuch).

7. Subcontractors (additional data processors)

7.1 The use of subcontractors as additional data processors is only permissible if the Client has given its prior consent.

7.2 A subcontractor relationship requiring consent exists if the Contractor commissions additional contractors to perform all or part of the services agreed in the Contract. The Contractor enters into agreements with these third parties to the extent necessary to ensure appropriate data protection and information security measures.

7.3 The Client agrees that the Contractor may commission subcontractors. Before commissioning or replacing the subcontractors, the Contractor informs the Client (if applicable, deadline and/or provision for emergency situations).

7.4 The Client may object to the change within a period of 2 days for good cause. If no objection is made within this period, the consent to the change is deemed given. If there is good cause under data protection law and if it is not possible for the parties to find an amicable solution, the Client is granted a special right of termination.

7.5 If the Contractor places orders with subcontractors, the Contractor is responsible for transferring its obligations under data protection law from this Contract to the subcontractor.

8. Confidentiality

8.1 The contracting parties are obliged to treat as confidential the information made available to them under this Contract by the respective other party as well as knowledge which they acquire in the course of this cooperation on matters – for example of a technical, commercial or organizational nature – from the respective other contracting party and not to exploit or use it or make it available to third parties during the term and after termination of this Agreement without the prior written consent of the party concerned. Any use of such information is limited solely to the use for the performance of this Contract.

8.2 This confidentiality obligation does not apply to information that

- was already generally known at the time of conclusion of the Contract or
- subsequently became generally known without any breach of the obligations contained in this Contract.

8.3 The contracting parties also impose the confidentiality and data protection obligations they have entered into on any and all persons or companies commissioned by them within the framework of the cooperation.

9. Liability and compensation

The Client and the Contractor are liable to data subjects in accordance with the provision set out in Art. 82 of the GDPR.

10. Information obligations, written form requirement, choice of law

10.1 Should the Client's data in the Contractor’s possession be endangered by attachment or seizure, by insolvency proceedings or composition proceedings or by other events or measures of third parties, the Contractor informs the Client thereof without undue delay. The Contractor immediately informs any and all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Client as the controller within the meaning of the General Data Protection Regulation.

10.2 Amendments and supplements to this Annex and all of its components – including any assurances made by the Contractor – require a written agreement, which may also be in an electronic format (text form), and the express indication that it is an amendment or supplement to these terms and conditions. This also applies to any waiver of this formal requirement.

10.3 In the event of any contradictions, the provisions of this Annex on data protection take precedence over the provisions of the Contract. Should individual parts of this Annex be invalid, this does not affect the validity of the remaining parts of the Annex.

10.4 German law applies.

10.5 The place of jurisdiction is the Contractor's registered office in Nuremberg.

11. Severability clause

11.1 Should individual provisions of this Agreement prove to be invalid or unenforceable in whole or in part, or become invalid or unenforceable as a result of changes in legislation after conclusion of the Agreement, the remaining provisions of the Agreement and the validity of the Agreement as a whole remain unaffected.

11.2 The invalid or unenforceable provision is replaced by a valid and enforceable provision which comes as close as possible to the meaning and purpose of the invalid provision.

11.3 If the Agreement proves to be incomplete, the provisions are deemed to be agreed which correspond to the meaning and purpose of the Agreement and would have been agreed if they had been considered.

12. Countersignature

Client

_____

First name, Last name

Title

_____ _____

(Signature of the client) (Place, Date)

resmio GmbH as **Contractor**

Tim Drüppel,

resmio GmbH

_____ Nuremberg, XX.XX.202X

(Signature of the Contractor) (Place, Date)

ANNEX 1

Technical and organizational measures for data security pursuant to

ART. 32 (1) B) OF THE GDPR

As part of the daily operations of resmio GmbH, the technical and organizational measures described below have been taken in accordance with the General Data Protection Regulation. These measures reflect the current status. They are subject to technical progress and further development.

1. Confidentiality (Art. 32 (1) b) of the GDPR)

Physical access control

Physical access control system:

- A key is required to access resmio's offices.
- All services are hosted by external providers. The API back end and the database are hosted by an external provider with appropriate user control that prevents access by third parties.
- Customers, employees without access authorization, external parties, suppliers and cleaning staff therefore have no access to the server room, as it is outsourced and managed externally.

System access control, especially data storage media control

User management:

- Appropriate system access controls have been implemented in the software to ensure that users (restaurant owners, waiters, ...) cannot access other users' data.

Passwords:

- When employees leave the company, their personalized accounts are locked.

Storage control

Storage control is intended to prevent unauthorized persons from accessing stored personal data and from entering, modifying and erasing such data.

- Authorizations in the IT systems are defined by the system administrators.

User control

User control is intended to prevent unauthorized persons from using automated processing systems by means of data transmission.

- All persons have signed agreements to ensure the confidentiality of information and data. External personnel (“freelancers”) do not have access to data from production systems.
- All external service providers have signed appropriate DPAs (Data Processing Agreements) to ensure data protection.
- Authorizations of departing employees are blocked when there are departing employees.
- Encryption technology is so far only used on the website. Transport Layer Security (**TLS**), more widely known by its former term Secure Sockets Layer (**SSL**),

is a hybrid encryption protocol for secure data transmission on the Internet, recognizable by https, rather than http in the URL.

Data access control

Data access control is intended to ensure that those authorized to use an automated processing system only have access to the personal data covered by their access authorization.

- Definition of authorizations in the IT systems
- Management of rights by system administrators
- Number of system administrators is reduced to the “bare minimum”
- Appropriate system access controls have been implemented in the software to ensure that users (restaurant owners, waiters, ...) cannot access other users' data.

2. Integrity (Art. 32 (1) b) of the GDPR)

Transmission control

Transmission control is intended to ensure that it is possible to verify and determine to which entities personal data has been or may be transmitted or made available using data transmission equipment.

- Users are restricted according to the principle of least privilege. The right to modify data is granted only to internal IT personnel. No external personnel (“freelancers”) have access to data from production systems.

Transport control

Transport control is intended to ensure that the confidentiality and integrity of data are protected during the transmission of personal data as well as during the transport of data storage media.

- The website is encrypted (TLS/SSL certificate).

3. Availability and resilience (Art. 32 (1) b) of the GDPR)

Restorability

Restorability is intended to ensure that deployed systems can be restored in the event of a failure.

- The system is built on Heroku's cloud infrastructure.

- Heroku has a high-availability infrastructure.

- There are automatic backups configured to back up all data on a daily basis.

  The backup is encrypted and automatically backs up daily; backup variants run autonomously and independently of the server and server-side backup. In the event that the server backup fails, or the server fails, the data can be restored.

  - Retention periods/retention: 4 days

Reliability

Reliability is intended to ensure that all system functions are available and any malfunctions that occur are reported.

- Independently functioning systems that enable data recovery.

- Automated reporting of malfunctions

Availability control

Availability control is intended to ensure that personal data are protected against destruction or loss.

- All services are hosted by external providers. The API back end and the database are hosted by an external provider with appropriate availability control.
- Heroku uses automatic fire detection and suppression systems and smoke detection sensors in all data center environments, mechanical and electrical infrastructure rooms, cold rooms, and generator equipment rooms.
- Heroku's data center power systems are designed to be fully redundant and can be maintained 24 hours a day, seven days a week without impacting operations. Uninterruptible power supply units provide backup power to critical and essential equipment in the facility in the event of a power outage. Data centers use generators to provide backup power for the entire facility.
- Heroku uses air conditioning to maintain a constant operating temperature for servers and other hardware, preventing overheating and reducing the possibility of operational failures.
- Monitoring of the system is performed by the Head of IT, Pavel Goltsev.

  Monitoring is the supervision of processes. It is an umbrella term for all types of systematic recording (logging), measurement or observation of an operation or process by means of technical aids or other observation systems.

  One purpose of monitoring is to determine whether an observed procedure or process is taking the desired course and whether certain threshold values are being met, in order to be able to intervene if this is not the case. Monitoring is therefore a special type of logging.

Monitoring is done with the software Cronitor, Uptime Robot, Heroku, Coralogix and Sentry.

The system can therefore be externally monitored by Heroku; the monitoring is to be performed at regular intervals.

4. Procedures for regular testing, assessment and evaluation (Art. 32 (1) d) of the GDPR; Art. 25 (1) of the GDPR)

Data protection - data security

Data protection and data security are among the most important prerequisites. Any and all measures are subject to regular monitoring to ensure that the state of the art is maintained.

Data protection by default (Art. 25 (2) of the General Data Protection Regulation)

It is ensured that only those personal data are collected that are necessary for the respective processing purpose.

Control of the data processors

Separate agreements are concluded with the individual data processors of resmio GmbH. No standardized contracts are signed in this case. The data processing is carried out taking into account the special nature of resmio GmbH and in particular with regard to the IT-critical infrastructures.

ANNEX 2

Sub-processors used by the Contractor

(April 2024)

Consent to the use of the bottom-mentioned sub-processo(s for the bottom-mentioned activities to be performed is granted, provided that the data protection requirements in accordance with this Agreement are also complied with in this contractual relationship (Sub-Processor DPA).

Sub-Processor Name	Permitted Sub-Processor Activities	CEO	Adress
Adyen N.V.	Payment services	Pieter van der Does	Simon Carmiggeltstraat 6-50, 1011 DJ Amsterdam, Niederlande
Stripe Inc.	Payment services	Patrick Collision	510 Townsend Street, San Francisco, CA 94103, USA

Amazon Web Services	On-demand provision of cloud resources for content delivery (content delivery network) of our SaaS offer	Jeff Bezos	410 Terry Avenue North, Seattle WA 98109, United States
GetResponse	Web analytics, newsletter distribution, newsletter success measurement	Simon Grabowski	Arkonska 6/A3, 80-387 Gdansk, Polen
Intercom	Provision of a live chat service within the web application for any support requests from customers	Eoghan McGabe	55 2nd Street, 4th floor, San Francisco, CA 94105, USA
Google LLC	Website & application analytics (via Google Analytics / Google Tag Manager), internal communication via e-mail and GSuite Office	Sundar Pichai	1600 Amphitheatre Pkwy, Mountain View, CA 94043, USA
Odoo S.A.	Deploy a cloud-powered CRM system to manage sales, marketing, customer care, and accounting	Sébastien Bruyr	Chaussée de Namur 40, 1367 Ramillies, Belgien
rapidmail GmbH	Dispatch of informal, non-promotional newsletters to resmio customers	Sven Kummer	Augustinerplatz 2, 79098 Freiburg, Deutschland

Sendgrid Inc.	Provision of a service for the automated dispatch of e-mail notifications from the system (e.g. booking notifications to restaurateurs / waiters)	Sameer Dholakai	1801 California Street, Suite 500, Denver, Colorado 80202, USA
Salesforce.com Inc.	Hosting / data storage of the web application Capture and logging of software errors for analysis and optimization purposes (Sentry) Caching of data to handle computationally intensive background processes (CloudAMQP) Provision of a general login solution (Coralogix)	Adam Gross	The Landmark @ One Market Street, Suite 300**,** San Francisco, CA 94105, USA
Vonage B.V.	Automated SMS dispatch, e.g. as a service for notifications about incoming reservations	David Jaarsma	Prins Bernhardplein 200, 1097 JB, Amsterdam, Niederlande