DATA PROCESSING AGREEMENT

Standard Contractual Clauses pursuant to Article 28(3) of Regulation 2016/679 (the GDPR)

between

The legal entity accepting the Opally Terms of Service (hereinafter the "Controller")

and

Opally ApS
CVR-no. DK45976904
Tyrolsgade 19, 4th,
2300 Copenhagen,
Denmark
(hereinafter the ”Processor”)

Each a "Party" and collectively the "Parties".

1. Contents

2. Preamble

1. These Clauses set out the rights and obligations of the Processor when processing personal data on behalf of the Controller.

2. These Clauses are designed to ensure the Parties' compliance with Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation/GDPR).

3. In connection with the provision of the Opally SaaS Solution, the Processor processes personal data on behalf of the Controller in accordance with these Clauses.

4. These Clauses shall take precedence over any similar provisions contained in other agreements between the Parties.

5. Four Appendices are attached to these Clauses and form an integral part hereof.

6. These Clauses shall not exempt the Processor from obligations to which the Processor is subject pursuant to the General Data Protection Regulation (GDPR) or other legislation.

3. Rights and Obligations of the Controller

1. The Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24), the applicable EU or Member State data protection provisions and these Clauses.

2. The Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The Controller shall be responsible for ensuring that there is a legal basis for the processing of personal data aimed at instructing the Processor to perform such processing.

4. The Processor Acts According to Instructions

1. The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject.

2. Such instructions shall be specified in Appendices A and C. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with these Clauses.

3. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

5. Confidentiality

1. The Processor shall only grant access to the personal data being processed on behalf of the Controller to persons under the Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis.

2. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn if access is no longer necessary, and personal data shall consequently no longer be accessible to those persons.

3. The Processor shall, at the request of the Controller, demonstrate that the persons concerned are subject to the above confidentiality.

6. Security of Processing

1. Article 32 of the GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

2. The Controller shall evaluate the risks to the rights and freedoms of natural persons posed by the processing and implement measures to mitigate those risks.

3. According to Article 32 of the GDPR, the Processor shall also – independently from the Controller – evaluate the risks to the rights and freedoms of natural persons posed by the processing and implement measures to mitigate those risks. To this effect, the Controller shall provide the Processor with all information necessary to identify and evaluate such risks.

4. Furthermore, the Processor shall assist the Controller in ensuring compliance with the Controller's obligations pursuant to Article 32 of the GDPR, by inter alia providing the Controller with information concerning the technical and organizational measures already implemented by the Processor pursuant to Article 32 of the GDPR pursuant to Appendix C.

7. Use of Sub-Processors

1. The Processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The Processor has the Controller's general authorization for the engagement of sub-processors. The Processor shall inform the Controller in writing of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor.

3. The list of sub-processors already authorized by the Controller can be found in Appendix B.

   Where the Processor engages a sub-processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in these Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of these Clauses and the GDPR.

4. The Processor shall remain fully liable to the Controller for the performance of the sub-processor’s obligations.

8. Transfer of Data to Third Countries or International Organizations

1. Any transfer of personal data to third countries or international organizations by the Processor shall only occur on the basis of documented instructions from the Controller and shall always take place in compliance with Chapter V of the GDPR.

2. In case transfers to third countries or international organizations, which the Processor has not been instructed to perform by the Controller, is required under EU or Member State law to which the Processor is subject, the Processor shall inform the Controller of that legal requirement prior to processing, unless that law prohibits such information on important grounds of public interest.

3. The Controller’s instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V of the GDPR on which the transfer is based, shall be set out in Appendix C.6.

9. Assistance to the Controller

1. Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III of the GDPR.

2. The Processor shall furthermore assist the Controller in ensuring compliance with the Controller's obligations pursuant to Articles 32 to 36 of the GDPR (Security, Breach Notification, Data Protection Impact Assessments) taking into account the nature of processing and the information available to the Processor.

3. The details regarding the assistance to be provided by the Processor are specified in Appendix C.

10. Notification of Personal Data Breach

1. In case of any personal data breach, the Processor shall, without undue delay after having become aware of it, notify the Controller of the personal data breach.

2. The Processor’s notification to the Controller shall, if possible, take place within 48 hours after the Processor has become aware of the breach to enable the Controller to comply with the Controller’s obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 of the GDPR.

3. The Processor shall assist the Controller in notifying the personal data breach to the competent supervisory authority, meaning the Processor is required to assist in obtaining the information listed in Article 33(3) of the GDPR.

11. Erasure and Return of Data

1. On termination of the provision of personal data processing services, the Processor shall be under obligation to return all the personal data to the Controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12. Audit and Inspection

1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and these Clauses and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

2. The procedures applicable to the Controller's audits, including inspections, of the Processor and sub-processors are specified in Appendices C.7 and C.8.

3. The Processor is required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Controller's and Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Processor's physical facilities on presentation of appropriate identification.

13. The Parties' Agreement on Other Terms

1. The Parties may agree other clauses concerning the provision of the personal data processing service e.g. liability, as long as they do not contradict directly or indirectly these Clauses or prejudice the fundamental rights or freedoms of the data subject.

14. Liability

1. The Processor's liability for any claim arising out of or in connection with this Data Processing Agreement shall be subject to the limitations of liability and liability caps set forth in the terms and conditions.

15. Commencement and Termination

1. This Data Processing Agreement is accepted by the Controller and becomes binding upon the Controller's acceptance of the Opally Terms of Service (e.g., by clicking "I Agree" or creating an account).

2. Both Parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. These Clauses shall apply for the duration of the provision of personal data processing services.

16. Contact persons

For the Controller (Customer): The primary contact person for the Controller shall be the account owner identified by the email address registered in the Opally platform.

For the Processor (Opally): Name: Gustav Søgård Title: Founder Phone number: +45 28 66 22 46 E-mail: gustav@opally.com

The Parties must notify each other of changes regarding contact persons (e.g., by updating the account profile or via email).

Appendix A Information about the processing

A.1. The purpose of the Processor's processing of personal data on behalf of the Controller:

The purpose is to enable the Supplier (Opally) to provide an AI-powered email assistant service to the Customer, which generates personalized email drafts for guest communication. The purpose extends to providing a website chatbot that assists visitors on the Customer's website 24/7 by answering questions and showing live prices/availability to increase direct bookings.

A.2. The Processor's processing of personal data on behalf of the Controller shall mainly concern (the nature of the processing):

- Collection/receipt of personal data from the Customer's PMS and email clients (via integration).
- Collection of data entered by visitors in the chatbot widget or via the Call Assistant.
- Storage of this personal data on secured servers.
- Analysis and processing using AI models to generate email drafts and responses.
- Deletion or return of personal data upon termination of the agreement.

A.3. The processing includes the following types of personal data about data subjects:

- Name (first and last name)
- Contact details (email address, phone number)
- Information voluntarily provided by the visitor in the chat/email dialogue
- Reservation details (booking number, dates, room number)
- Preferences or specific requests related to the stay
- Content of email correspondence between Customer and guest

A.4. The processing includes the following categories of data subjects:

- The Customer's guests (past, present, and potential).
- Visitors to the Customer's website interacting with the chatbot.

A.5. Duration of the processing:

The processing commences when these Clauses enter into force and continues as long as user is on active subscription.

Appendix B Authorized sub-processors

B.1. Approved Sub-Processors

By the commencement of these Clauses, the Controller authorizes the engagement of the following sub-processors:

NAME	LOCATION	DESCRIPTION OF PROCESSING
Microsoft Corporation	One Microsoft Way, Redmond, WA 98052, USA	Cloud infrastructure & Azure OpenAI. Data stored in EU regions.
Supabase	San Francisco, CA 94101, USA	Database & Storage. Data Center: Frankfurt (EU).
OpenAI	3180 18th Street, San Francisco, CA 94110, USA	AI Processing via API.
Vercel, Inc.	440 N Barranca Avenue #4133, Covina, CA 91723, USA	Web App Hosting. Data Center: Frankfurt (EU).
Intercom, Inc.	55 2nd Street, 4th Floor, San Francisco, CA 94105, USA	Customer communication platform (Chat/Email).
Amplitude, Inc.	201 Third Street, Suite 200, San Francisco, CA 94103, USA	Product Analytics.
Stripe, Inc.	354 Oyster Point Blvd, South San Francisco, CA 94080, USA	Payment Processing.
Resend	548 Market St, PMB 95233, San Francisco, CA 94104, USA	Transactional Emails.
ElevenLabs, Inc.	169 Madison Ave #2484, New York, NY 10016, USA	AI Voice Generation (Call Assistant).
Twilio Inc.	101 Spear St FL 5	Telephony Infrastructure.

NAME	LOCATION	DESCRIPTION OF PROCESSING
	San Francisco, CA 94105	
Google LLC	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	AI Models.
Exa Labs, Inc.	375 Alabama Street Suite 410, San Francisco CA 94110, USA	Providing AI-powered search and data processing API.
Cloudflare, Inc.	101 Townsend St, San Francisco, CA 94107, USA	CDN, Security & DDoS Protection.

B.2. Notice period for authorization of sub-processors

The Processor shall inform the Controller of any planned changes with at least 30 days' notice.

Appendix C Instruction pertaining to the use of personal data

C.1. Subject matter/instruction

The Processor is instructed to process personal data only to the extent necessary to provide the Opally SaaS Solution.

C.2. Security of Processing

The level of security shall reflect:

The processing involves general personal data regarding guests and communication data. The risk to the rights and freedoms of the data subjects is assessed to be moderate, as a personal data breach could lead to loss of control over own data, damage to reputation, or other significant disadvantages for the data subjects. It is crucial to ensure the confidentiality, integrity, and availability of the personal data. There is no indication of processing of special categories of personal data (sensitive data) pursuant to Article 9 of the GDPR.

The Processor is entitled and obliged to make decisions regarding which technical and organizational security measures shall be implemented to establish the necessary (and agreed) security level.

However, the Processor shall – under all circumstances and as a minimum – implement the following measures, which have been agreed with the Controller:

- **Pseudonymization and encryption of personal data:**
  - Personal data shall be pseudonymized where technically feasible and appropriate.
  - All personal data shall be encrypted during transmission (in transit) using recognized encryption protocols (e.g., TLS 1.2+).
  - All personal data shall be encrypted during storage (at rest) in databases and file storage systems using industry-standard encryption algorithms.
- **The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services:**
  - Access to systems processing personal data shall be based on the "least privilege" principle and the "need-to-know" principle.
  - Access control systems with strong passwords and two-factor authentication (2FA) shall be used for all administrative access.
  - Firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) shall be implemented to protect network interfaces.
  - Vulnerability scans and penetration tests shall be performed regularly.
- **The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:**
  - A comprehensive backup system shall be established with regular backups of all personal data.
  - Backups shall be stored securely, geographically separated, and encrypted.
- **Procedures for regular testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing:**
  - Regular internal and/or external security audits shall be performed to assess compliance with security policies and standards.
  - The Supplier shall have a process for continuously monitoring and assessing the threat landscape and updating security measures accordingly.

  - Employees processing personal data shall receive regular training in information security and data protection.
- **Access to data via the internet:**
  - Access to the Solution and underlying systems via the internet shall be secured with encrypted connections (HTTPS/TLS) and strong authentication mechanisms.
  - Secure API access points and keys shall be used for integration with the Customer's PMS and email clients.
- **Protection of data during transmission:**
  - All data transfers between the Customer's systems and Opally, as well as between Opally and its sub-processors, shall occur via encrypted channels (e.g., TLS/SSL).
- **Protection of data during storage:**
  - Data shall be stored in secured data centers complying with recognized security standards (e.g., ISO 27001).
  - Access to stored data shall be limited to authorized personnel with a clearly defined need.
- **Use of home/remote workstations:**
  - Employees working remotely shall use secure VPN connections to access the company's network and systems.
  - Clear policies shall be in place regarding the use of own devices (BYOD) and the security of home workstations, including protection against unauthorized access to devices with access to personal data.
- **Logging:**
  - All relevant access, changes, and processing activities in systems containing personal data shall be logged.
  - Log files shall be secured against manipulation, stored for an appropriate period, and reviewed regularly to detect irregularities.

C.3 Assistance to the Controller

The Processor shall, as far as possible, assist the Controller in accordance with Clause 9.1 and 9.2.

Scope, extent, and costs of assistance: The Processor's assistance is provided to support the Controller's fulfilment of its obligations under the GDPR. Assistance that can be provided via the Solution's standard functionality (e.g., for export and deletion of data) is included in the Agreement. Requests from the Controller requiring significant manual case handling or technical development by the Processor (estimated at more than 2 hours per case) will be considered a separate service. Such service will be invoiced subject to the Controller's prior written approval based on the Processor's current hourly rate of €55 EUR. This does not apply if the assistance is required due to the Processor's breach of the Agreement.

Specific technical and organizational measures:

1. **Assistance with the exercise of data subjects' rights (cf. Clause 9.1):**
   - *Technical assistance: Provide features in the Solution supporting the Controller in locating, exporting, or deleting data regarding specific data subjects.*
   - *Organizational assistance: Provide guidance and support helping the Controller navigate the Solution to accommodate requests.*
   - *Forwarding of requests: Forward any request from data subjects received directly by the Processor to the Controller without undue delay.*
2. **Assistance with personal data breaches (cf. Clause 9.2.a and 10):**
   - *Notification: Notify the Controller in accordance with the agreed time limits.*

   - *Information for reporting: Provide relevant and available information regarding the breach, including, if possible, the nature of the breach, number of affected persons, probable consequences, and measures taken.*
   - *Documentation: Maintain an internal record of all personal data breaches.*
3. **Assistance with Data Protection Impact Assessments (DPIA) and prior consultations (cf. Clause 9.2.c and 9.2.d):**
   - *Availability of information: Make available relevant information regarding the Solution's functions, security measures, and data processing procedures necessary for the Controller's execution of a DPIA.*

C.4 Storage Period/Erasure Routine

Personal data processed by the Processor on behalf of the Controller is stored for as long as the Opally SaaS Solution is in force between the Parties.

Upon termination of the service regarding the processing of personal data, the Processor shall return all personal data to the Controller and delete existing copies, in accordance with Clause 11.1. The Processor shall confirm to the Controller that all relevant personal data has been deleted.

Deletion of data will take place no later than 30 days after completed return of data to the Controller, unless longer storage is required under Union or Member State law.

The Processor maintains internal procedures ensuring that personal data is deleted or anonymized when it is no longer necessary for the purpose of the processing or to comply with legal requirements.

C.5 Place of Processing

Processing of the personal data covered by these Clauses cannot be performed at other locations than the following without the Controller's prior written approval:

- **Primary locations (The Processor's own facilities/office):**
  - **Address:** Tyrolsgade 19, 4th, 2300 Copenhagen S, Denmark
  - **Used by:** Opally ApS
- **Sub-processors' locations:**
  - **Microsoft Corporation:**
    - **Location:** EU (Primarily Azure regions in Europe, e.g., Sweden Central or West Europe). USA (only for support and administration).
    - **Used by:** Microsoft Corporation (as sub-processor for cloud infrastructure and AI processing via Microsoft Foundry/Azure).
  - **Supabase:**
    - **Location:** EU (Frankfurt, Germany - eu-central-1).
    - **Used by:** Supabase (as sub-processor for data storage and database functionality).
  - **OpenAI:**
    - **Location:** USA (San Francisco, CA)
    - **Used by:** OpenAI (as sub-processor for AI processing and generation of email drafts).
  - **Vercel Inc.:**
    - **Location:** EU (Frankfurt, Germany)
    - **Used by:** Vercel Inc. (as sub-processor for hosting of web application and handling of web logs for the Solution).
  - **Intercom, Inc.:**
    - **Location:** USA (San Francisco, CA)

        - **Used by:** Intercom, Inc. (as sub-processor for customer communication platform and support, including chat and email).
    - **Amplitude, Inc.:**
        - **Location:** USA (San Francisco, CA)
        - **Used by:** Amplitude, Inc. (as sub-processor for user behavior and product analytics).
    - **ElevenLabs Inc.:**
        - **Location:** USA (New York, NY)
        - **Used by:** ElevenLabs Inc. (as sub-processor for AI generation for calls).
    - **Twilio Inc.:**
        - **Location:** USA (San Francisco, CA)
        - **Used by:** Twilio Inc. (as sub-processor for call infrastructure).
    - **Google LLC:**
        - **Location:** USA
        - **Used by:** Google LLC (as sub-processor for AI processing and generation of AI models).
    - **Exa Labs, Inc.:**
        - **Location:** USA
        - **Used by:** Exa Labs, Inc. (as sub-processor for AI-powered search and data processing API).
    - **Cloudflare, Inc.:**
        - **Location:** USA (Headquarters) and EU.
        - **Used by:** Cloudflare, Inc. (as sub-processor for network security and performance).

C.6 Instruction on the Transfer of Personal Data to Third Countries
The Processor is instructed to transfer personal data to the USA to the extent necessary for the provision of the Opally SaaS Solution, and provided that a valid transfer basis pursuant to GDPR Chapter V is secured for each transfer.

Specific instruction and basis for transfer:
1. Transfers based on the EU Commission's Adequacy Decision (GDPR Art. 45)
Transfer of personal data to the following recipients in the USA takes place on the basis of the EU Commission's adequacy decision for the EU-U.S. Data Privacy Framework (DPF):

- **Recipients:**
    - Microsoft Corporation: Provision of cloud infrastructure and AI services. (Note: Data is stored and processed primarily in the EU, but transfer to the USA may occur in connection with support and maintenance, covered by DPF).
    - Vercel Inc.: For hosting of web application and handling of web logs.
    - Intercom, Inc.: For customer communication platform and support.
    - Amplitude, Inc.: For user behavior and product analytics.
    - Stripe, Inc.: For payment processing and subscription management.
    - Resend: For sending of system emails (transactional emails).
    - Twilio Inc.: For handling of call infrastructure.
    - Google LLC: For AI processing and generation of AI models (Gemini).
    - Cloudflare, Inc.: For provision of web security, hosting, DDoS protection, and CDN services.

Processor's obligation: The Processor commits to ensuring that these sub-processors maintain their active certification under the DPF scheme throughout the duration of the agreement. The Processor shall, upon request from the Controller, be able to document the sub-processor's active certification.

2. Transfers based on Standard Contractual Clauses (GDPR Art. 46)
Transfer of personal data to the following recipients in the USA takes place on the basis of the EU Commission's Standard Contractual Clauses (SCCs):

- **Recipients:**
  - OpenAI: For AI processing and generation of email drafts.
  - ElevenLabs Inc.: For AI generation for calls.
  - Exa Labs, Inc.: For AI-powered search and data processing API.
- **Processor's obligation:** The Processor guarantees to have entered into valid SCCs with OpenAI. The Processor shall, upon request from the Controller, make a copy of the entered SCCs available to the Controller as documentation that the necessary transfer basis is established.

General
If the Controller does not in these Clauses or subsequently provide a documented instruction regarding transfer of personal data to a third country, the Processor is not entitled within the framework of these Clauses to perform such transfers.

C.7 Procedures for the Controller's Audits, including Inspections, of the Processing of Personal Data Entrusted to the Processor
The Processor acknowledges the Controller's right to audit to demonstrate compliance with the GDPR and this Agreement.
The Processor aims to obtain a recognized, independent third-party audit report (e.g., ISAE 3000) to document its security level.
Until such an external report is available, the Processor shall, upon request, provide the Controller with access to its internal documentation for compliance with the security measures described in Appendix C.2.

C.8 Procedures for Audits, including Inspections, of the Processing of Personal Data Entrusted to Sub-processors
The Processor is responsible for ensuring that sub-processors used in connection with the provision of the Services comply with the same data protection obligations as those appearing in this Data Processing Agreement, cf. Clause 7.3.

To demonstrate compliance with sub-processors' obligations, the following applies:

- Audit reports from third parties: The Processor commits to obtaining and retaining relevant documentation (e.g., ISAE 3000 Type 2, ISAE 3402 Type 2 reports, ISO 27001 certifications, or similar third-party audit reports) from its sub-processors. This documentation confirms the sub-processor's compliance with applicable data protection legislation and the agreed security standards.
- Availability to the Controller: The Processor will, upon written request from the Controller, make relevant documentation regarding sub-processors' compliance available to the Controller for review. This does not, however, include commercially confidential information in sub-processors' agreements.
- Processor's responsibility for supervision: The Processor has the primary responsibility for supervising its sub-processors. The Controller's potential wish for direct inspection at a sub-processor shall be coordinated via the Processor and can only take place with the Processor's prior written approval and on terms ensuring confidentiality and the sub-processor's operations. Any costs associated with such direct inspection shall be borne by the Controller.