AGREEMENT

ON PROCESSING OF PERSONAL DATA
ON BEHALF OF A CONTROLLER

– hereinafter referred to as “Agreement” –

between

(Controller)
(address)

– hereinafter referred to as “Controller” –

and

Haiilo (Entity)
(address)

– hereinafter referred to as “Processor” –

Hereinafter referred to individually and collectively as the “party” or” parties”

1. Legal basis, subject matter, duration of agreement

1) This Agreement is based on the provisions of the EU General Data Protection Regulation (GDPR).
2) This Agreement governs the collection and processing of Personal Data by the Processor for and on behalf of the Controller, according to the Controller's instructions, in connection with the respective terms of the cloud services. Purpose of the processing is the provision and management of the software as well as its securing according to the data processing description in **Annex 1**. The scope and nature of Personal Data processing as well as categories of data subjects also arise from **Annex 1**.
3) This Agreement shall be valid for the duration of the existence of a processing purpose in accordance with paragraph 2 of this section, unless otherwise stated in the following provisions. The right of extraordinary termination for important reasons remains unaffected. If the parties entered into a data processing agreement or other similar agreements before, the parties acknowledge and agree that this Agreement shall supersede and replace prior data processing agreements as of the effective date.

2. Rights and obligations of the controller

1) The Controller is, within the frame of this Agreement, responsible for the compliance with the legal provisions of the data protection laws, in particular the lawfulness of data transfer to the Processor as well as the safeguarding of the rights of the data subjects.
2) The Processor shall process Personal Data only on documented instructions from the Controller – also in regard to the transmission of Personal Data to a third country or an international organization – as long as the Processor is not obliged to process by law of the European Union or member states, he is subject to. In the latter case the Processor informs the Controller about the legal requirements before processing, unless the relevant law prohibits such because of substantial public interest. Changes in processing object and procedure are to be agreed upon and documented jointly. If the Processor believes that an order given by the Controller infringes against data protection provisions, he shall immediately inform the Controller. The Processor has the right to suspend such an order until it gets confirmed or changed by the Controller. The Processor has the right to refuse an evidently illegal order.
3) The Processor will authorize only reliable personnel with sufficient qualification with the processing. In particular, the Processor shall oblige the personnel, who are involved in the processing of Personal Data of the Controller, to maintain data and telecommunication secrecy and shall instruct them about the relevant obligations resulting from data processing and data protection provisions as well as existing instruction or purpose limitations.
4) The Processor has appointed a data protection officer who can be reached under dpo@haiilo.com or +49 40 609 4000 70. In case of a change of the data protection officer the Controller will be informed immediately.
5) Both parties support one another promptly and comprehensively in case of possible data protection violations, defense of claims from data subjects or third parties and defense of penalties by supervisory authorities. In particular, the Processor supports the Controller to comply with art. 32 to 36 GDPR and his obligation to answer requests from data subjects based on their rights referred to in chapter III GDPR.
6) Upon written request, the Processor shall provide the Controller, within a reasonable period of time, with all available information and evidence required for the assessment of the contractual conformity of the data processing. In order to verify the compliance of the data protection provisions in this Agreement before the processing and in regular intervals thereafter, in particular the agreed technical

and organizational measures (see **Annex 2** of this Agreement) of the Processor and documents the results. The Controller can therefore e.g

a) obtain self-declarations from the Processor,
b) obtain a certificate from an expert or
c) after prior notification in good time within the normal business hours and without disruption of the operating process personally or by a qualified third party, which shall not be in competition with the Processor, satisfy itself from the compliance of agreed provisions.

The Processor shall inform the Controller in text immediately in case of suspicion of violation of contractual obligations by itself or by for the processing employed personnel or any other violations against data protection provisions.

3. Technical and organizational measures

1) The Controller and Processor implement appropriate technical and organizational measures ("TOM") to ensure the safety of the Controller's data and avoid their misuse and abuse, so an adequate level of protection according to data protection law – in particular GDPR – can be reached.
2) From the parties for the purposes of this Agreement found as appropriate TOM, are described in **Annex 2.**
3) TOM are subject to technological progress and development. The Processor is insofar permitted to implement alternative adequate measures. He hereby has to guarantee that the level of data protection does not fall below the one of this Agreement. Crucial changes must be agreed on and documented.

4. Return and deletion

The Processor shall at the choice of the Controller either completely and irrevocably delete, or return all data entrusted to him by the Controller, including all hard copies and data carriers, unless the Processor is obliged to store the data by law of the European Union or the Federal Republic of Germany. This also covers possible tests or scrap material. If the Controller requests the return of its data, the parties will agree upon further modalities of the return (e.g. form, deadline).

5. Sub-Processors

1) The services agreed upon in this Agreement are also provided with the Sub-Processors listed in **Annex 3**. The Processor is within the frame of this Agreement authorized to employ further Processors (Sub-Processors).
2) The Processor selects Sub-Processors carefully based on their suitability and reliability. The Processor shall oblige the Sub-Processor according to this Agreement. The Processor shall inform the Controller on its written behalf about the data protection obligations of the Sub-Processor, including if necessary and to the extent legally valid, insight into relevant agreements.
3) The Processor informs the Controller by e-mail of any intended order and/or change in respect of the inclusion or change of a Sub-Processor. It may proceed as suggested if the Controller raises no objection because of an important reason within 14 days upon receipt of the information.
4) Sub-Processors are also Processors of the Sub-Processor (Sub-Sub-Processors). Subcontracting relationships within the meaning of this Agreement shall not be deemed to include orders placed by the Processor with third parties to assist in the execution of the order and which do not include any processing services of data of the Controller. Not a sub-contractual relation in regard to this Agreement are in particular ancillary services, which provide e.g. telecommunication, post or transport

services, maintenance and user service or disposal of data carrier as well as other measures for safeguarding the confidentiality, accessibility, integrity and capacity of hard- and software of data processing systems.

5) For any transfer of personal data outside of the EEA Processor shall provide sufficient guarantees in accordance with art. 44 ff. GDPR such as by the adoption of standard contractual clauses adopted by the European Commission in accordance with Article 46(2) of Regulation (EU) 2016/679 in its version dated 4th of June 2021.

6. Liability

1) For the compensation of any damages, data subjects may suffer from an incorrect or unlawful processing after GDPR or other relevant data protection provisions within the frame of this Agreement, the Controller shall be liable in relation to the data subject. In such cases, the Controller has the right to claim regress from the Processor for such a damage, as long as obligations of this Agreement have been violated.
2) The parties make each other exempt from claims from third parties, if one party provides proof that it is not responsible in any way for the circumstances leading to the damage for the data subject.

7. Miscellaneous

1) This data processing Agreement substitutes all previous processing provisions.
2) The invalidity of a provision of this Agreement shall not affect the validity of the remaining provisions. If a provision proves invalid, the parties shall replace it with a new provision which approximates the intentions of the parties as closely as possible.
3) For Controllers located within the EU, German law including EU law such as the GDPR shall apply, with the place of jurisdiction being Hamburg, Germany.
4) For Controllers located outside of the EU, this Agreement shall be governed by and construed in accordance with the relevant laws of the Controller's registered address. The parties acknowledge and agree that any disputes arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the competent courts in the Controller's jurisdiction.
5) Any changes to this Agreement and any side agreements shall be made in writing. This shall also apply to the waiver of this written form clause itself.
6) For the purposes of this Agreement, the Data Protection Officer ("DPO") can be contacted at the following email address: dpo@haiilo.com. The Controller may provide the contact information of their relevant DPOr by sending an email to the designated address mentioned above.

ANNEXES

The following annexes are integral parts of this Agreement:

Annex 1: Details about data processing

Annex 2: Technical and organizational measures

Annex 3: Approved Sub-Processors

For the Processor	**For the Controller**
Place, Date	Place, Date
Signature	Signature
Name	Name
Role	Role

Annex 1

Details about data processing

1. Purpose of the processing

The main tasks performed by the Processor are as follows:

- Provisioning of the software, which mainly enables its users to collaborate and communicate while offering various functionalities.
- Hosting of data from the Controller on an IT-infrastructure provided by the Processor and its Sub-Processors.
- Processing of personal data through feedback and opinions from participants for research, decision-making, and improvement purposes.

2. Categories of data subjects, data types, access methods

a. Categories of data subjects:
In general, the software serves the communication among employees. If intended by the Controller to process further categories of data subjects, it would have to indicate those in the following:

_____

b. Affected personal data:
The following data types will be processed:

- Surname/First name
- Profile data (e.g. telephone, e-mail)
- User content and interactions
- IP address
- Metadata

If intended by the Controller to use further data types, it should mark those in the following:

_____

c. Sensitive data / special categories of data within the meaning of Art. 9 GDPR:
For the usage of the software no sensitive data is required. If it is intended by the Controller to process sensitive data in the software, this data must be specified in detail here:

_____

d. Access to personal data

The Processor provides services in the area of hosting, maintenance, remote maintenance or IT fault analysis. It cannot be ruled out that the Processor gains access to data thereby. Hence, following obligations apply:

- Testing and maintenance work on workstations at the Controller shall be carried out upon approval by the relevant authorized individual/affected employee of the Controller.
- A separate notification (by e-mail/in writing) about imminent test and maintenance work is sent to the Controller by the Processor before the beginning of the work.
- Upon request of the Controller, the Processor shall provide information about which tasks will be performed when and by which employees of the Processor, and how these persons shall identify and authenticate themselves to the Controller.
- The Processor shall make use of the access rights granted to it in such a way – including with regard to timing – that is necessary for the proper performance of the commissioned maintenance and testing tasks.

Annex 2

Technical and organizational security measures

1. **Organization of Information Security**

Objective:

Haiilo has established and endorsed an information security department, backed by business leadership, to ensure that our personnel possess the necessary skills and knowledge in information security.

Measures include:

a) Haiilo employs personnel who are fully dedicated to information security on a full-time basis.
b) Haiilo has a Security Steering Committee that is formed from various departments to tackle information security concerns across different aspects of the business.
c) The information security personnel reports directly to the executive management.
d) Haiilo implements a set of comprehensive security policies, approved by the senior management and communicated within the company.
e) All staff members have signed confidentiality agreements that have been legally reviewed and are applicable during and after their employment period.
f) Non-compliance with information security policies by personnel employed at Haiilo may result in disciplinary actions and lead to sanctions, including dismissal.
g) All staff members receive routine information security training through various mediums such as videos, interactive training, posters and announcements. They are required to undergo and pass an information security quiz during the onboarding process and subsequently on a quarterly basis. Additionally, all personnel undergo data privacy training during onboarding. Staff members in specialized technical roles participate in role-specific security training tailored to their tasks.
h) The information security management system is committed to continual reviewals and improvements.

2. **Information Security Management System**

Objective:

Haiilo has implemented an Information Security Management System (ISMS) to assess risks related to the security of clients and personnel data, to oversee the evaluation and mitigation of these risks, and to consistently enhance its information security measures.

Measures include:

a) Haiilo has implemented an ISMS to handle security matters in a professional manner. Both Haiilo and its ISMS undergo regular review/audits conducted by an independent external auditor, and they are certified according to ISO/IEC 27001:2022 as well as SOC2 Type II or a later version.
b) SOC 2 Type II and ISO/IEC 27001:2022 are global standards outlining <criteria for setting up, executing, sustaining, and enhancing an ISMS, encompassing the evaluation and mitigation of information security risks. A copy of our ISO27001 certificate and our SOC 2 attestation report can be shared upon request via trust.haiilo.com.

3. **Physical Access**

Objective:

Haiilo's data processing systems are exclusively accessed by authorized users who have been authenticated.

Measures include:

a) Haiilo operates its products from ISO-Family including ISO27001 certified and SOC2 accredited third party cloud hosting providers. The data centers have well-defined and protected physical security boundaries, robust access control policies, controlled delivery and loading zones, surveillance systems, and 24/7 security personnel. Only authorized personnel have access to the premises of these data centers.
b) Power and telecommunication cables transporting personnel data or supporting information services at the data centers are safeguarded against interception, interference, and damage.
c) Data centers have implemented physical protection measures against natural disasters, malicious attacks and accidents.
d) The data centers maintain an emergency power failure backup plan which ensures that data centers continue to function seamlessly in the event of a power outage.
Read more about the Data and Security of the data centers here.
e) Haiilo utilizes the use of keyfobs and safety locks to access the office premises, all Haiilo offices are equipped with CCTVs at main doors.

4. System Access

Objective:

Access to Personal Data and Haiilo's internal systems are strictly controlled and safeguarded in accordance with industry best practices.

Measures include:

a) Access to Haiilo's internal systems is restricted to personnel of Haiilo, with access strictly restricted as per need-to-know principle and limited as required to perform and accomplish their tasks.
b) All user access to all company systems related to Haiilo is linked to a unique identifier (UserID) to ensure traceability of actions at all times.
c) Haiilo utilizes the use of Single-Sign-On (SSO) whenever possible.
d) Haiilo implements a password policy that prohibits unauthorized sharing of passwords and mandates password change in case of a compromise. All passwords must meet specified minimum requirements and are stored in encrypted form within a password management system (1Password). Additionally, each endpoint device has a password protected screensaver that is initiated after 5 minutes of inactivity.
e) Haiilo enforces Multi-Factor authentication via the identity provider (IdP) for accessing all systems within Haiilo.
f) Haiilo has a comprehensive process for deactivating user accounts and revoking their access upon a member's departure from the company, or adjusting access rights if their role changes.
g) Haiilo deploys appropriate firewall technologies inline with the industry standards to safeguard the various applications, servers, and virtual machines from web-based attacks at the data centers.
h) Haiilo offers a wide range of authentication capabilities, including ability for customers to set their own password policies and support for SAML 2.0 and OpenID. Customers have the option to connect different user directories such as Active Directory, LDAP, and LDAPS. User directories can be connected via Google Workspace or Microsoft graph as well if customer desire.

5. Data Access

Objective:

Authorized individuals accessing data processing systems are granted access only to specific personal data they are authorized to access.

Measures include:

a) Haiilo restricts personnel access to data and systems based on the "need-to-know" principle.

b) Haiilo implements a formal background verification process during the screening call on all necessary documents. For personnel in Prospective C-level, VP-level, and information security a certificate of good conduct is required.
c) Onboarding training covers access rights and general principles regarding the definition and utilization of personal data.
d) Haiilo employs data pseudonymization/anonymization where appropriate and practical to reduce the likelihood of inappropriate access to Personal Data. Haiilo offers a sovereign cloud solution consisting of an external key management operated by a reliable third party provider.
e) The production environment used for Haiilo products is separate from the development and testing environment. The test environment uses anonymized production data, ensuring that customer data is not included in test data.
f) All end user devices at Haiilo are safeguarded by anti-malware software (MalwareBytes) and is included in a Mobile Devices Management System (MDM) where a set of policies are enforced. In addition, all end-user devices are monitored by an Endpoint Detection and Response Software (Nebula).
g) The network within Haiilo offices is protected by a firewall to enhance security measures.

6. Data Transmission

Objective:

Ensure that unauthorized parties are unable to access, copy, modify, or delete customer data during transmission.

Measures include:

a) Customer access to Haiilo products is protected by TLS 1.2 or higher.
b) Haiilo utilizes strong encryption methods to all other transmission of Personal Data to external networks.

7. Development Process

Objective:

Haiilo enforces both administrative and technical measures to guarantee secure code development.

Measures include:

a) Haiilo employs a defense in depth approach to software development and uses a Secure Development Lifecycle (SDLC) that includes a wide range of security testing, bug reporting and management procedures.
b) Haiilo provides training to its software developers, engineers and quality assurance that encompasses development best practices and emerging security threats related to application security and secure coding.
c) Security testing involves conducting peer code review, conducting unit tests, integration tests, API tests, End-to-end (E2E) testing and functional testing.
d) All modifications to the code are conducted through a regulated and approved release mechanism, operating within a structured change control program. This program tracks, documents, and approves change requests prior to being implemented.
e) Haiilo conducts third-party penetration testing on the various platforms, assessing them against emerging application security threats. Identified vulnerabilities are promptly addressed to maintain the platform's robust security posture.
f) All encryption and other cryptographic functionalities used within Haiilo products follow industry standards as per BSI, NIST standards and ISO/IEC.

8. Availability

Objective:

Personal Data is safeguarded against destruction or loss, and there are measures in place to ensure timely access, restoration, or availability of customer data in case of an incident.

Measures include:

a) Haiilo implements redundancy measures to enhance availability and resilience of the cloud infrastructure. The cloud utilizes redundant components, such as load balancers and virtual machine instances to ensure high availability.
b) Data centers have power failure recovery plans, generators on-site are in place to ensure that the data center is safeguarded against power outages.
c) Data centers are monitored around the clock for power, network, environmental and technical issues.
d) Haiilo generates encrypted backup copies of customer data on a daily basis, the data is stored in a location with different availability zones than the primary data center. Haiilo implemented measures to promptly identify backup failures and regularly conduct restoration tests to ensure effectiveness and completeness of backups.
e) Haiilo abides by a Business Continuity Plan and a Disaster Recovery Plan that are regularly reviewed and updated.
f) Haiilo conducts regular testing of components within the Business Continuity Plan and Disaster Recovery Plan, the review/practice drill is aimed to enhance the process.

9. Data Separation

Objective:

Personal Data belonging to each customer is consistently kept separate from the data of other customers through logical or physical separation.

Measures include:

a) Haiilo designs its systems to guarantee the separation, whether logical or physical, of the Personal Data originating from different customers.
b) At every stage of processing, customer data obtained from various customers can be distinguished, ensuring that the data is consistently separated either physically or logically.

10. Incident Management

Objective:

In case of any security breach involving customer data, efforts are made to minimize the impact of the breach, and the customer is notified promptly.

Measures include:

a) Haiilo implements an Incident Handling Policy and a Vulnerability Management Process detailing roles and responsibilities, as well as procedures for evaluating and categorizing information security events as incidents.
b) Haiilo has configured monitoring and logging systems in the cloud infrastructure to generate records of system and application events.
c) Haiilo maintains a synchronized clock on all systems to facilitate investigations in case of an incident.
d) In the event of a Personal Data breach that requires notification according to applicable laws, Haiilo will notify the customer without undue delay. In addition, Haiilo will as well notify the competent supervisory authority without undue delay and within the applicable statutory notice. The notification to both the customer and the authorities will include where required by applicable law the description

of the nature of the Personal Data Breach and the possible consequences. Haiilo shall take reasonable, necessary measures to mitigate the effects of the Personal Data Breach.

11. Compliance

Objective:

Haiilo engages in third-party audits to evaluate the efficacy of both technical and administrative controls incorporated within conducted measures, benchmarking them against industry-standard security frameworks.

Measures include:

a) Haiilo undergoes regular internal and external security audits
b) Haiilo maintains a documented policy for overseeing supplier security, the policy encompasses criteria for assessing and approving suppliers, as well as measures conducted to monitoring and evaluating the performance of the suppliers.
c) Haiilo implements regular application vulnerability scans and external annual penetration testing on the various products within Haiilo using reputable third party service providers. Further details can be shared upon request.

Annex 3

Approved Sub-Processors

The following Sub-Processors can be deployed within the scope of this Agreement:

Sub-processor 1	**Google Cloud EMEA Limited**, 70 Sir John Rogerson's Quay, Dublin 2, Ireland
Data Protection Officer	https://support.google.com/policies/answer/9581826
Services	Hosting provider
Processing Location	EU (for US customers: USA)
Legal Basis	Data Processing Agreement ("DPA"), EU-US Data Privacy Framework certified, EU Standard Contractual Clauses ("SCC")

Sub-Processor 2	**T-Systems International GmbH**, Hahnstraße 43d, 60528 Frankfurt, Germany
Data Protection Officer	datenschutz@telekom.de
Services	Sovereign cloud external key management
Processing Location	Germany
Legal Basis	DPA

Sub-Processor 3	**Telekom Deutschland GmbH**, Landgrabenweg 151, 53227 Bonn, Germany
Data Protection Officer	datenschutz@telekom.de
Services	Email gateway
Processing Location	EU
Legal Basis	DPA

Sub-Processor 4	**Zendesk Inc.**, 109 Market Street, San Francisco CA 94103, USA
Data Protection Officer	privacy@zendesk.com
Services	SaaS servicedesk ticket system
Processing Location	European Economic Area (EEA)
Legal Basis	DPA, EU-US Data Privacy Framework certified, SCC

Sub-Processor 5	**Other Haiilo Group entities**
Data Protection Officer	dpo@haiilo.co

Services	Customer support
Processing Location	Germany, UK, USA, Finland (depending on local entity)
Legal basis	DPA, SCC

(Sub-Processor 6)	**Gainsight Inc.**, 350 Bay Street, Suite 100, San Francisco, CA 94133, USA
Data Protection Officer	privacy@gainsight.com
Services	Learning platform (part of the Haiilo Academy; **use is optional**)
Processing Location	USA
Legal Basis	DPA, EU-US Data Privacy Framework certified, SCC

Additionally for Customers of the product **Haiilo Align – Employee Communications:**

Sub-Processor 7	**ImageKit Inc.**, Christiana Corporate Business Center, 200 Continental Drive, Suite 401, Newark, DE 19713, USA
Data Protection Officer	support@imagekit.io
Services	Content delivery network (optimised media delivery)
Processing Location	Germany
Legal Basis	DPA, EU-US Data Privacy Framework certified, SCC

Sub-Processor 8	**Twilio Inc.**, 375 Beale Street Suite 300 San Francisco, CA 94105, USA
Data Protection Officer	privacy@twilio.com
Services	Email sending/delivery service
Processing Location	USA
Legal Basis	DPA, EU-US Data Privacy Framework certified, SCC