(English Translation Only)

The translation below is provided for your convenience only. If there is any discrepancy between the translation in English and the original Japanese text (including due to the delay in translation), the original Japanese text takes precedence.

Data Processing Appendix

This Data Processing Appendix ("DPA") is an integral part of HENNGE One Terms of Service (the “Terms”) and governs the processing of Personal Data by HENNGE (the “Processor”) on behalf of Customer (the “Controller”) as part of HENNGE One services (the “Service”) provided by the Processor to the Controller pursuant to the Terms. Unless otherwise defined herein, capitalized terms shall have the meanings set out in the Terms. In the event of any conflict between the provisions of this DPA and the Terms, the provisions of this DPA shall prevail.

Article 1 Definitions

1. "Applicable Data Protection Laws” means the legislation protecting the right to privacy with respect to the processing of Personal Data applicable to the processing under this DPA, including, but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) of the European Parliament and of the Council of 27 April 2016 (“GDPR”), the Data Protection Act 2018 (“DPA 2018”), the UK General Data Protection Regulation (having the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018) (“UK GDPR”), and the Act on the Protection of Personal Information (Act No.57 of May 30, 2003, “APPI”).
2. "Data Subject" means a natural person who can be identified, directly or indirectly, in particular by reference to an identification number, location data, an online identifier or to one or more factors specific to his/her physical, physiological, genetic, mental, economic, cultural or social identity (including without limitation, such information as will allow easy reference to other information and will thereby enable the identification of the specific individual), or as otherwise defined under Applicable Data Protection Laws.

3. "Personal Data" means any personally identifiable information relating to a specific Data Subject, or as otherwise defined under Applicable Data Protection Laws;
4. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, or as otherwise defined under Applicable Data Protection Laws.
5. "Processing/processing (of Personal Data) " means any operation or set of operations which is performed upon Personal Data by the Processor as part of the Services, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, or as otherwise defined under Applicable Data Protection Laws.

Article 2 Roles of the Parties and Details of the Processing

Details of the processing of Personal Data under this DPA shall be as follows and as set out in Annex 1:

Nature and purposes of the processing	As specified in column A
Subject matter of the processing	As specified in column B
Categories of Data Subjects	As specified in column C
Type of Personal Data	As specified in column D
Duration of the processing	As specified in column E

Article 3 Obligations and Rights of the Controller

1. The Controller shall be responsible for assessing the lawfulness of the processing of Personal Data and for implementing measures for the protection of the rights of Data Subjects.
2. If either Party incurs any costs, expenses, or damages (including those arising from claims made by third parties, including Data Subjects, in connection with this DPA

and those arising from the processing of Personal Data based on instructions from the other Party) in the performance of its obligations and responsibilities under this DPA, and the cause of such costs, expenses, or damages is attributable to the other Party, the first Party may claim reimbursement from the other Party for such costs, expenses, and damages. The same shall apply to any costs, expenses, or damages incurred by either Party because of measures taken by a supervisory authority in connection with this DPA.

Article 4 Obligations and Rights of the Processor

1. The Processor shall have the following obligations:
   (1) to process the Personal Data only in accordance with Controller's documented instructions which are as set forth in the Terms and this DPA as may be amended from time to time, including with regard to transfers of Personal Data to a third country or an international organization ("Cross-border data transfer"), unless required to do so by applicable law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless the applicable law prohibits such informing on important grounds of public interest;
   (2) to ensure that the Processor's personnel authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The Processor shall ensure that its personnel access Personal Data only to the extent necessary for the purposes of performing the processing activities under this DPA;
   (3) to take Specific Organizational and Technical Security measures set out in Annex 2, in accordance with Article 7 of this DPA;
   (4) to comply with the conditions set out in Article 5 of this DPA, when engaging other processors;
   (5) to assist the Controller by appropriate technical and organizational measures (including but not limited to, forwarding requests for exercising rights received from Data Subjects promptly to the Controller) insofar as this is possible taking into account the nature of the processing, for the fulfilment of

the Controller’s obligation to respond to Data Subjects’ requests to exercise their rights set out under Applicable Data Protection Laws;

(6) to assist the Controller in ensuring compliance with the Controller’s obligations under the Applicable Data Protection Laws taking into account the nature of processing and the information available to the Processor. In particular, where the Processor becomes aware that a Personal Data breach has occurred in relation to Personal Data processed under this DPA, the Processor shall, taking into account the nature of processing and the information available to the Processor, without undue delay, notify the Controller of such Personal Data breach and assist the Controller in meeting the Controller’s notification and communication obligations under Applicable Data Protection Laws;

(7) to delete all the Personal Data covered by this DPA (including any copies thereof) after the end of the Service, unless applicable laws require continued storage of the Personal Data. The Processor shall ensure ongoing compliance with this DPA until such deletion occurs;

(8) appoint a Data Protection Officer;

(9) exercise necessary and appropriate supervision over their employees (including contract employees and subcontractors engaged in the business of Processor or affiliated companies of Processor, regardless of the form of contract) when allowing them to handle Personal Data, in order to ensure the safe management of such Personal Data;

(10) provide or disclose Personal Data to third parties only when permitted under Applicable Data Protection Laws; and

(11) if Processor is required by Applicable Data Protection Laws, to make available to the Controller all information necessary to demonstrate compliance with the obligations set out in this article Article 4 and allow for and contribute to audits including reasonable inspections conducted by the Controller or another auditor mandated by the Controller. Before the commencement of any audit, the Parties shall mutually agree on the scope, timing and duration of the audit as well as on the reimbursement by Controller of Processor’s costs arising from the audit.

2. The Processor shall inform the Controller if, in its opinion, an instruction from the Controller may violate Applicable Data Protection Laws.

Article 5 Processing by Sub-processors

1. The Processor has the general authorization of the Controller to engage third parties (hereinafter "Sub-processor") listed in column F of Annex 1and if applicable, the Sub-processors listed on the Sub-processors list published on the Processor's website. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors. When informing the Controller, the Processor shall provide the information necessary for the Controller to exercise its right to object, including the name of the Sub-processor. The Controller may object in writing to the engagement of a Sub-processor within ten business days of receipt of the notification from the Processor of the engagement of the Sub-processor.
2. Where the Processor engages a Sub-processor for carrying out specific processing activities on behalf of the Controller, data protection obligations no less protective than the obligations set out in this DPA shall be imposed on the Sub-processor by way of a contract or other legal act. Where the Sub-processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the Sub-processor's obligations.
3. Where the engagement of a Sub-processor triggers a Cross-border data transfer, the Processor shall take necessary measures to comply with the regulations governing such Cross-border data transfer under the Applicable Data Protection Laws.
4. The Sub-processor listed in column F of Annex 1 and on the Sub-processor list published on the Processor's website may be engaged in the processing of the Personal Data. The Processor represents that it has selected such Sub-processors with due care, in particular in relation to the appropriateness of their technical and organizational measures. The Controller approves the use of such Sub-processor, subject to compliance with paragraphs 2 through 4 of this Article.

Article 6 Processing under the Authority of the Processor

The Processor shall ensure that any person acting under its authority and having access to Personal Data shall process such Personal Data only upon instructions from the Controller as set out in this DPA or in the Terms, unless required by law.

Article 7 Specific Technical and Organizational Security Measures

1. The Processor shall implement appropriate technical and organizational measures including the following to ensure the appropriate security level to the risk to be caused by the processing of Personal Data:
    (a) pseudonymization and encryption of Personal Data;
    (b) ensuring confidentiality, integrity, availability and resilience of processing systems and Services;
    (c) ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
    (d) establishment and implementation of processes for regularly testing and assessing the effectiveness of technical and organizational measures in order to ensure the security of processing.
2. The technical and organizational measures to be implemented by the Processor in accordance with paragraph 1 are as set out in Annex 2.
3. Technical and organizational measures shall be reviewed and updated as necessary in accordance with the development and improvement of technology. Therefore, in order to ensure that such measures keep providing the appropriate level of security, the Processor shall conduct periodic reviews and, if necessary, take measures in addition to, or instead of, the those set out in Annex 2.
4. To demonstrate the implemented technical and organizational measures to the Controller, the Processor may, at its discretion, provide certifications, reports or extracts from reports issued by independent bodies (e.g., auditor, internal auditor, data protection officer, IT security department, data protection auditor, quality auditor) or appropriate certifications from IT security department or data protection auditor.
5. In addition to the technical and organizational measures described in the preceding four paragraphs, the Processor shall implement security measures from both physical and human perspectives, and shall review and update them as necessary.

6. The Processor shall, at the written request of the Controller, provide the Controller with the information necessary to respond to that request regarding the obligations of the Processor. The Processor shall reasonably cooperate in good faith with the supervisory authority or the Controller in the event of an inspection required under applicable laws.

Annex 1 to DPA: Details of the Processing of Personal Data

A	**Nature and purposes of the processing**	● To provide the Service as agreed between Processor and Controller. ● To optimize the Service performance and enhance reliability through monitoring and analyzing Service usage. ● To monitor, analyze, examine, and investigate all the data and log data which are provided and/or transmitted by Controller through the Service if Processor determines that it is necessary to do so from maintenance, operational, or technical purposes. Below is applicable to Tadrill users: ● To confirm and analyze the contents of reports regarding targeted attack emails. ● To create a list to be provided to Controller of individuals to receive training service for targeted attack emails. Processor shall not provide or disclose the accessed information to any third party.
B	**Subject matter of the processing**	● Data related to authentication and authorization when the Service and other cloud services via the Service are accessed. ● Content and metadata of emails, attachments, and shared files sent and received by Controller systems and users. ● System logs, event logs, and audit logs generated through the use of the Service. Below is applicable to Tadrill Users: ● Personal Data contained in third party services such as Gmail provided by Google LLC, including the name and email address of senders and receivers (including CC and BCC), email contents such as header, subject and body of the email,
C	**Categories of the Data Subjects**	● Internal parties of the Controller, such as the Controller's employees and sub-contractors. ● External parties of the Controller

		and user information such as Tadrill user's name, email address and organizational unit to which the user belongs.
D	**Type of Personal Data**	● Identification, authentication, and contact information ○ Name, email address, any other related information input by admin. ● Communication and content information ○ Emails, attachments, files. ● Security and operations-related information ○ Access logs, audit logs, action logs etc. ● IP address ● Tracking ID (amplitude, Google Analytics) ● Device ID ● MAC address ● Other information obtained by use of Cookies
E	**Duration of processing**	Unless otherwise specified, data processing shall cease upon the termination or expiration of the Service provision to Controller.
F	**Sub-processor**	**1. Amazon Web Services Japan G.K.** a. 3-1-1 Kamiosaki, Shinagawa-ku, Tokyo 141-0021 Japan **2. Datadog, Inc.** a. 620 8th Ave 45th Floor, New York, NY 10018 USA **3. Functional Software, Inc. doing business as Sentry** a. 45 Fremont Street, 8th Floor, San Francisco, CA 94105 USA **4. Salesforce** a. Salesforce Tower, 1-1-3 Marunouchi, Chiyoda-ku, Tokyo 100-0005, Japan **5. Hubspot** a. 2 Canal Park, Cambridge, MA 02141, United States **6. Zendesk** a. San Francisco, California, USA (specifically, 181 S. Fremont Street, San Francisco, CA 94105) **7. Statuspage** a. Level 6, 341 George Street, Sydney, NSW 2000, Australia **8. WithSecure K.K.** a. Tokyo Sankei Building 27F, 1-7-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan **9. Cybertrust** a. Toranomon Kotohira Tower, 1-2-8 Toranomon, Minato-ku, Tokyo 105-0001, Japan **10. ngrok** a. 548 Market St PMB 26741, San Francisco, CA USA **11. Anyflow**

		a. Dai-5 Kano Building 5F, 3-26-16 Shibuya, Shibuya-ku, Tokyo 150-0002, Japan

Annex 2 to DPA: Technical and Organizational Measures

1. Access Control to Buildings and Facilities

To prevent unauthorized physical access to buildings and facilities where personal data is processed, the following measures are implemented:

- Access control systems
- ID readers, magnetic cards, IC chip cards, and company-issued smartphones
- All doors are secured
- Surveillance systems
- Alarm systems and video/television displays
- Log records of entries and exits from the facilities

2. Access Control of Systems

To prevent unauthorized access to IT systems, the following measures, including user identification and authentication, are implemented:

- Passwords with requirements for the use of special characters, minimum length, and regular changes
- Prohibition of the access of guest users and anonymous accounts
- Centralized access management to systems using HENNGE Access Control
- Access to IT systems requiring approval by IT department

3. Access Control to Data

To prevent authorized users from accessing data beyond their authorization, the following measures are implemented:

- Distinction of access permissions
- Access permissions defined according to job responsibilities
- Automatic recording of user access logs via HENNGE Access Control

4. Control of Data Transfers

To prevent unauthorized access, modification, or deletion of data during transfers, and to ensure secure and documented transfers, the following measures are implemented:

- All data transfers are conducted using secure tools such as HENNGE Email DLP, HENNGE Secure Transfer, and HENNGE Secure Download
- HTTPS communication is mandatory for remote access, and all data transfers and communication are encrypted using HENNGE Access Control

5. Input and Processing Control

To maintain records of data management and maintenance activities, and to ensure traceability of data modifications and deletions, the following measures are implemented:

- Log records of user activities across all HENNGE One services implemented within the company.

6. Operational Control

To ensure that data processing is carried out strictly in accordance with the instructions of the data controller, the following measures are implemented:

- Clear, written contract-based instructions based on ISMS 27001 and ISO 27018 certified qualifications.
- Monitoring of compliance with contract

7. Availability Control

To protect data against accidental damage or loss, the following measures are implemented:

- Backups
- Uninterruptible power supplies in preparation for blackout
- Business Continuity Plan
- Off-site storage
- Antivirus system and firewall system

8. Separation Control

To process data collected for different purposes separately, the following measures are implemented:

- Limiting access to data stored for different purposes according to job responsibilities

- Separation of access permissions for each business IT system using HENNGE Access Control
- Separation of IT test and production environments