Gustave CONNECT

Data Processing Addendum

In order that you as a service user and data controller (referred to as "Controller" or "User") may use or continue to use the Gustave Connect service ("Services") offered by us, Gustave Connect ("Gustave Connect" or "we", "us"), and our registered address is Schiemond 20, 3024EE, Rotterdam, NL and data processor (referred to as "Gustave Connect" or "Processor"), you agree that certain Personal Data you submit as part of your use of our Services and these data processing terms ("Terms") shall apply (notwithstanding any other terms and conditions applicable to the delivery of the Services to the contrary) in order to address the compliance obligations imposed upon Gustave Connect and its Users pursuant to Applicable Law.

1. DEFINITIONS

1.1. "Affiliate" means an entity that, directly or indirectly, controls, is controlled by, or is under common control with a Party. As used herein, "control" means the power to direct the management or affairs of an entity and the beneficial ownership of fifty percent (50%) or more of the voting equity securities or other equivalent voting interests of an entity.

1.2. "Applicable Law(s)" means all US, UK, and EU laws, regulations, and other legal or regulatory requirements relating to privacy, data protection/security, or the Processing of Personal Data applicable to Gustave Connect's performance of its services under the Agreement,including without limitation the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. ("CCPA") as amended by the California Privacy Rights Act of 2020 ("CPRA"), including any implementing regulations, the United Kingdom Data Protection Act 2018, and the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), Turkey`s Data Protection Law 6698 ("DPL") and the Dutch GDPR Implementation Act (Uitvoeringswet Algemene Verordening gegevensbescherming) ("UAVG").

1.3. "User Contact Data" means the User's contact information.

1.4. "User Personal Data" means User Data, as defined in the Agreement, consisting of Personal Data, except for User Contact Data.

1.5. "EEA" means, for purposes of this DPA, the European Economic Area (which is composed of the member states of the European Union), Norway, Iceland, Liechtenstein, and Switzerland.

1.6. "EU SCCs" means the Standard Contractual Clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described in Section 9.

1.7. "Personal Data Breach" means the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to User Personal Data.

1.8. "Personal Data" includes "personal data," "personal information," and "personally identifiable information," each as defined by Applicable Law.

1.9. "Process" and "Processing" mean any operation or set of operations performed on Personal Data, or on sets of Personal Data, whether or not by automated means, such as collecting, recording, organizing, creating, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing (by transmission, dissemination or otherwise making such data available), aligning or combining, restricting, erasing, or destroying such Personal Data.

1.10. "Standard Contractual Clauses" means the EU SCCs or the UK SCCs, as applicable.

1.11. "UK SCCs" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, available as of the Effective Date at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/ and completed as described in Section 9.

Gustave CONNECT

Data Processing Addendum

2. RELATIONSHIP OF THE PARTIES

2.1. User is the Controller as defined under Applicable Laws, and User determines the means and purposes for which User Personal Data is Processed by Gustave Connect. To the extent Gustave Connect Processes User Personal Data subject to Applicable Laws, Gustave Connect is a Processor and Service Provider as defined under Applicable Laws, and Gustave Connect will Process the User Personal Data according to the instructions set forth in this DPA, the Agreement, and as required under Applicable Laws. User and Gustave Connect are independent Controllers, as defined under Applicable Laws, with respect to User Contact Data. Either Party may Process User Contact Data as necessary for the purpose of (i) carrying out its obligations under the Agreement, (ii) applicable legal or regulatory requirements, (iii) requests and communications with the other Party, (iv) administrative, business, and marketing purposes, and (v) to protect its respective rights in accordance with applicable law and, in the case of Gustave Connect, maintaining the security and integrity of the Services.

2.2. Gustave Connect hereby certifies that it understands the restrictions and obligations set forth in this DPA in relation to its role as a Processor and Service Provider, and that it will comply with them.

3. USER'S INSTRUCTIONS TO GUSTAVE CONNECT

3.1. Purpose Limitation. Gustave Connect will not

3.1.1. sell or share (as defined by CCPA) User Personal Data,

3.1.2. Process User Personal Data for any purpose other than for the specific purposes set forth in the Agreement,

3.1.3. retain, use, or disclose any such data outside of the direct business relationship between the Parties,

3.1.4. combine any User Personal Data with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, except as otherwise permitted by Applicable Law, or

3.1.5. otherwise engage in any Processing of User Personal Data beyond that in which a Processor may engage under the Applicable Law or in which a Service Provider may engage under the Applicable Law, unless obligated to do otherwise by Applicable Law. In such a case, Gustave Connect will inform User of the applicable legal obligation before engaging in the Processing, unless legally prohibited from doing so. Further details regarding Gustave Connect's Processing operations are set forth in Schedule 1. To the extent User discloses or makes available deidentified data (as such term is defined under Applicable Law) within the User Data to Gustave Connect, Gustave Connect shall not attempt to re-identify such data.

3.2. Lawful Instructions. User will not instruct Gustave Connect to Process User Personal Data in violation of Applicable Law. Gustave Connect will without undue delay inform User if, in Gustave Connect's opinion, an instruction from User infringes Applicable Law. The Agreement, including this DPA, constitutes User's complete and final instructions to Gustave Connect regarding the Processing of User Personal Data, including for purposes of the Standard Contractual Clauses. User shall also have the right to take reasonable and appropriate steps to stop or remediate any unauthorized Processing of User Personal Data by Gustave Connect.

4. LIMITATIONS ON DISCLOSURE

Gustave Connect will not disclose User Personal Data to any third party without first obtaining User's written consent, except as provided in Section 5, Section 7 or Section 9,

except as required by law. Gustave Connect will require all employees, contractors, and agents who Process User Personal Data on Gustave Connect's behalf to protect the confidentiality of the User Personal Data and to comply with the other relevant requirements of this DPA.

5. SUBCONTRACTING

5.1. Sub-Processors. Gustave Connect may subcontract the collection or other Processing of User Personal Data only in compliance with Applicable Law and any additional conditions for subcontracting set forth in the Agreement. User acknowledges and agrees that Gustave Connect's Affiliates and certain third parties may be retained as sub-processors to Process User Personal Data on Gustave Connect's behalf (under this DPA as well as under the Standard Contractual Clauses, if they apply) in order to provide the Services. Gustave Connect's third-party sub-processors are

5.1.1. Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany;

5.1.2. OpenAI OpCo, LLC, 575 Florida Street, San Francisco, CA 94110, United States;

5.2. Prior to a sub-processor's Processing of User Personal Data, Gustave Connect will impose contractual obligations on the sub-processor substantially the same as those imposed on Gustave Connect under this DPA to the extent applicable to the nature of the services provided by such sub-processor. Gustave Connect remains liable for its sub-processors' performance under this DPA to the same extent Gustave Connect is liable for its own performance.

5.3. Notification. Gustave Connect will provide Users with at least ten (10) days' written notice of new sub-processors before authorizing such sub-processor(s) to Process User Personal Data in connection with the provision of the Services. Gustave Connect will notify User at the email address provided in the signature block of this DPA for purposes of this notification. The sub-processor agreements to be provided under Section 5(j) of the EU SCCs may have all commercial information, or provisions unrelated to the EU SCCs, redacted prior to sharing with User, and User agrees that such copies will be provided only upon written request.

5.4. Right to Object. User may object to Gustave Connect's use of a new sub-processor on reasonable grounds relating to the protection of User Personal Data by notifying Gustave Connect promptly in writing within ten (10) business days after receipt of Gustave Connect's notice in accordance with the mechanism set out in Section 5.2. In its notification, User will explain its reasonable grounds for objection. In the event User objects to a new sub-processor, Gustave Connect will use commercially reasonable efforts to make available to User a change in the Services or recommend a commercially reasonable change to User's configuration or use of the Services to avoid Processing of User Personal Data by the objected-to new sub-processor without unreasonably burdening User. If Gustave Connect is unable to make available such change within a reasonable period of time, which will not exceed thirty (30) days, either Party may terminate without penalty the Processing of User Personal Data and/or the Agreement with respect only to those services which cannot be provided by Gustave Connect without the use of the objected-to new sub-processor by providing written notice to the other Party.

6. ASSISTANCE AND COOPERATION

6.1. Security. Gustave Connect will provide reasonable assistance to User regarding User's compliance with its security obligations under Applicable Law relevant to Gustave Connect's role in Processing User Personal Data, taking into account the nature of Processing and the information available to Gustave Connect, by implementing the technical and organizational measures set forth in Schedule 2, without prejudice to Gustave Connect's right to make future replacements or updates

to the measures that do not materially lower the level of protection of User Personal Data. Gustave Connect will ensure that the persons Gustave Connect authorizes to Process the User Personal Data are subject to written confidentiality agreements or are under an appropriate statutory obligation of confidentiality no less protective than the confidentiality obligations set forth in the Agreement.

6.2. Personal Data Breach Notification & Response. Gustave Connect will comply with the Personal Data Breach-related obligations directly applicable to it under Applicable Law. Taking into account the nature of Processing and the information available to Gustave Connect, Gustave Connect will inform User of a substantiated Personal Data Breach without undue delay or within the time period required under Applicable Law, and in any event no later than seventy-two (72) hours following such substantiation. Gustave Connect will notify User at the email address provided in the signature block of this DPA for purposes of Personal Data Breach notifications. Any such notification is not an acknowledgement of fault or responsibility. This notification will include Gustave Connect's then-current assessment of the following information, to the extent available, which may be based on incomplete information:

6.2.1. the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of User Personal Data records concerned;

6.2.2. the likely consequences of the Personal Data Breach; and

6.2.3. measures taken or proposed to be taken by Gustave Connect to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects.

6.3. Gustave Connect will provide timely and periodic updates to User as additional information regarding the Personal Data Breach becomes available. User is solely responsible for complying with legal requirements for incident notification applicable to User and fulfilling any third-party notification obligations related to any Personal Data Breach. Nothing in this DPA or in the Standard Contractual Clauses will be construed to require Gustave Connect to violate, or delay compliance with, any legal obligation it may have with respect to a Personal Data Breach or other security incidents generally.

7. DATA SUBJECT REQUESTS

To the extent legally permitted, Gustave Connect will without undue delay notify User if Gustave Connect receives any request from an individual seeking to exercise any right afforded to them under Applicable Law regarding their Personal Data (a "Data Subject Request"). To the extent User, in its use of the Services, does not have the ability to address a Data Subject Request, Gustave Connect will, upon User's request, take commercially reasonable efforts to assist User in responding to such Data Subject Request, to the extent Gustave Connect is legally permitted to do so and the response to such Data Subject Request is required under Applicable Law.

8. DPIAS AND CONSULTATION WITH AUTHORITIES

Upon User's written request, Gustave Connect will provide User with reasonable cooperation and assistance as needed and appropriate to fulfill User's obligations under Applicable Law to carry out a data protection impact assessment related to User's use of the Services. Gustave Connect will provide reasonable assistance to User in the cooperation or prior consultation with the Supervisory Authority (as defined under the GDPR) in the performance of its tasks relating to the data protection impact assessment, and to the extent required under the Applicable Law.

9. INTERNATIONAL DATA TRANSFERS

Data Processing Addendum

9.1. User authorizes Gustave Connect and its sub-processors to make international transfers of the User Personal Data in accordance with this DPA so long as Applicable Law for such transfers is respected.

9.2. With respect to User Personal Data transferred from the EEA, the EU SCCs will apply and form part of this DPA, unless the European Commission issues updates to the EU SCCs, in which case the updated EU SCCs will control. Undefined capitalized terms used in this provision will have the meanings given to them (or their functional equivalents) in the definitions in the EU SCCs. For purposes of the EU SCCs, they will be deemed completed as follows:

9.2.1. Where User acts as a Controller and Gustave Connect acts as User's Processor with respect to User Personal Data subject to the EU SCCs, Module 2 applies.

9.2.2. Where User acts as a Processor and Gustave Connect acts as User's sub-processor with respect to User Personal Data subject to the EU SCCs, Module 3 applies.

9.2.3. Section 7 (the optional docking Section) is not included.

9.2.4. Under Section 9 (Use of sub-processors), the Parties select Option 2 (General written authorization). The initial list of sub-processors is set forth at Section 5. Gustave Connect will provide notice of updates to that list at least ten (10) business days in advance of any intended additions or replacements of sub-processors, in accordance with Section 5 of this DPA.

9.2.5. Under Section 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body is inapplicable.

9.2.6. Under Section 17 (Governing law), the Parties select Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The Parties select the law of the Netherlands.

9.2.7. Under Section 18 (Choice of forum and jurisdiction), the Parties select the courts of Rotterdam.

9.2.8. Annexes I and II of the EU SCCs are set forth in Schedule 1 below.

9.2.9. Annex III of the EU SCCs (List of sub-processors) is inapplicable.

9.2.10. By entering into this DPA, the Parties are deemed to be signing the EU SCCs.

9.3. With respect to User Personal Data transferred from the United Kingdom for which the law of the United Kingdom (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the UK SCCs form part of this DPA and take precedence over the rest of this DPA as set forth in the UK SCCs, unless the United Kingdom issues updates to the UK SCCs, in which case the updated UK SCCs will control. Undefined capitalized terms used in this provision will have the meanings given to them (or their functional equivalents) in the definitions in the UK SCCs. For purposes of the UK SCCs, they will be deemed completed as follows:

9.3.1. Table 1 of the UK SCCs:

9.3.1.1. The Parties' details are the Parties and their affiliates to the extent any of them is involved in such transfer, including those set forth in Schedule 1.

9.3.1.2. The Key Contacts are the contacts set forth in Schedule 1.

9.3.2. Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 are the EU SCCs as executed by the Parties pursuant to this Addendum.

9.3.3. Table 3 of the UK SCCs: Annex 1A, 1B, and II are set forth in Schedule 1.

9.3.4. Table 4 of the UK SCCs: Either Party may terminate this Addendum as set forth in Section 19 of the UK SCCs.

9.4. By entering into this DPA, the Parties are deemed to be signing the UK SCCs and their applicable Tables and Appendix Information.

9.5. With respect to User Personal Data transferred from Switzerland for which Swiss law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the EU SCCs will apply and will be deemed to have the following differences to the extent required by the Swiss Federal Act on Data Protection ("FADP"):

9.6. References to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR.

9.7. The term "member state" in the EU SCCs will not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Section 18(c) of the EU SCCs.

9.8. References to Personal Data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope.

9.9. Under Annex I(C) of the EU SCCs (Competent supervisory authority): where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the EU SCCs insofar as the transfer is governed by the GDPR.

10. AUDITS

Gustave Connect will allow for and contribute to audits, including inspections, conducted by User or another auditor mandated by User subject to the following conditions: so long as the Agreement remains in effect, User may request that Gustave Connect provide it with Gustave Connect's most recent information security reports no more than once annually relating to Gustave Connect's compliance with this DPA (an "Audit"). To the extent User uses a third-party representative at User's sole expense to conduct the Audit, User will ensure that such third-party representative is bound by obligations of confidentiality no less protective than those contained in the Agreement. User will provide Gustave Connect with ninety (90) business days prior written notice of its intention to conduct an Audit. User will conduct the Audit in a manner that will result in minimal disruption to Gustave Connect's business operations and such Audit will take no longer than two (2) business days. Further, User will not be entitled to receive data or information of other Users of Gustave Connect or any other Confidential Information of Gustave Connect that is not directly relevant for the authorized purposes of the Audit.

11. LEGAL PROCESS

If Gustave Connect is legally compelled by a court or other government authority to disclose User Personal Data, then to the extent permitted by law, Gustave Connect will promptly provide User with sufficient notice of all available details of the legal requirement and reasonably cooperate with User's efforts to challenge the disclosure, seek an appropriate protective order, or pursue such other legal action, as Gustave Connect deems appropriate.

12. DESTRUCTION OF PERSONAL DATA

Upon termination of the Agreement and written request from User, Gustave Connect will delete or anonymize User Personal Data, unless prohibited by Applicable Law. Notwithstanding the foregoing, nothing will oblige Gustave Connect to delete or anonymize User Personal Data from files created for security, backup and business continuity purposes

sooner than required by Gustave Connect's data retention processes. Any User Personal Data that may be retained beyond the duration of the Agreement will still be protected in accordance with this DPA and Gustave Connect shall not process such User Personal Data except as strictly permitted under Applicable Law.

13. APPLICABILITY AND ORDER OF PRECEDENCE

This DPA replaces any existing data processing addendum the Parties may have previously entered into in connection with the Agreement. In the event of a conflict between the terms of the Agreement and this DPA, the terms of the DPA will apply. In the event of a conflict between this DPA and the applicable Standard Contractual Clauses, the Standard Contractual Clauses will apply.

SCHEDULE 1

Annexes I and II of the EU SCCs

1. List of Parties
    - 1.1.1. Module Two: Transfer Controller to Processor
    - 1.1.2. Module Three: Transfer Processor to Processor
    - 1.2. Data exporter(s):
        - 1.2.1. Name: The exporter is the User specified in the Agreement.
        - 1.2.2. Address: specified in the Agreement.
        - 1.2.3. Contact person's name, position and contact details: specified in the Agreement.
        - 1.2.4. Activities relevant to the data transferred under these Sections: Obtaining the Services from data importer.
        - 1.2.5. Role (Controller/Processor): Controller
    - 1.3. Data importer(s):
        - 1.3.1. Name: Gustave Connect, Schiemond 20, 3024EE, Rotterdam, NL;
        - 1.3.2. Address: specified in the Agreement.
        - 1.3.3. Contact person's name, position and contact details: specified in the Agreement.
        - 1.3.4. Activities relevant to the data transferred under these Sections: Providing the Services to data exporter.

Data Processing Addendum

1.3.5. Role (Controller/Processor): Processor

2. Description of Transfer
   - 2.1. Module Two: Transfer Controller to Processor
   - 2.2. Module Three: Transfer Processor to Processor
3. Categories of data subjects whose personal data is transferred
   - 3.1. Data subjects whose Personal Data is uploaded by data exporter to, or otherwise received directly or indirectly from data exporter by or through, the Services, or provided by data exporter to Gustave Connect to input into the Services.
4. Categories of personal data transferred
   - 4.1. The data exporter may transfer Personal Data to Apps Do Wonders, the extent of which is determined and controlled by the data exporter in its sole discretion. Such Personal Data may include any category of Personal Data the data exporter may enter into the Services.
   - 4.2. Sensitive data transferred and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
   - 4.3. In particular,
     - 4.3.1. Personal contact details
     - 4.3.2. Information relating to User inputs and User conversation
     - 4.3.3. Where applicable sensitive personal information
     - 4.3.4. Business contact details
     - 4.3.5. Online Identifier
     - 4.3.6. Location Data
     - 4.3.7. Identifier Information
5. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)
   - 5.1. Continuously, for the length of the Agreement between the Parties.
6. Nature of the processing
   - 6.1. User Personal Data transferred will be processed to (i) provide the Services to the data exporter and fulfill the data importer's obligations under the Agreement; and (ii) comply with applicable law.
7. Purpose(s) of the data transfer and further processing
   - 7.1. User Personal Data transferred will be processed to (i) provide the Services to the data exporter and fulfill the data importer's obligations under the Agreement; and (ii) comply with applicable law.
8. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
   - 8.1. User Personal Data will be retained for the length of time necessary to provide Services under the Agreement and in accordance with Gustave Connect's data retention processes and as otherwise required by applicable law.
9. For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing
   - 9.1. Gustave Connect's sub-processors will process User Personal Data to assist Gustave Connect in providing the Services pursuant to the Agreement, for as long as needed for Gustave Connect to provide the Services.
10. Competent Supervisory Authority
    - 10.1. Module Two: Transfer Controller to Processor
    - 10.2. Module Three: Transfer Processor to Processor
11. Identify the competent supervisory authority/ies in accordance with Section 13.
    - 11.1. The Parties will follow the rules for identifying such authority under Section 13 and, to the extent legally permissible, select the Autoriteit Persoonsgegevens,

Gustave CONNECT

Data Processing Addendum

Bezuidenhoutseweg 30, 2594 AV DEN HAAG, The Netherlands, (https://autoriteitpersoonsgegevens.nl/en).

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL MEASURES

Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data

1. Module Two: Transfer Controller to Processor
2. Module Three: Transfer Processor to Processor

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. ACCESS CONTROLS

1.1. Control Measures

1.1.1. Gustave Connect has implemented reasonable system access controls and physical access controls designed to limit access based on authorization and prevent personnel and others who should not have access from obtaining access to Gustave Connect systems housing User Data.

1.2. System Access Controls

1.2.1. Gustave Connect's system access control measures include the following:

1.2.1.1. restricting unauthorized users from accessing information not needed for their roles through role-based user access, and using "least privileged" principles;

1.2.1.2. unique user accounts identifiable to individual users, password requirements, and Auth0 authentication;

1.2.1.3. provisioning and removal of employee access to User Data when access is no longer required; and

Data Processing Addendum

1.2.1.4. periodic access reviews to ensure that only Gustave Connect personnel who still require access to User Data have such access.

1.3. Physical Access Controls

1.3.1. Gustave Connect utilizes cloud hosting infrastructure for the Services. All physical security controls are managed by the cloud hosting provider. Annually, Gustave Connect reviews the applicable security and compliance reports of its cloud hosting provider to ensure appropriate physical security controls, which include:

1.3.1.1. use of data centers with physical and environmental controls appropriate to the risk for User Data and for the equipment, assets, or facilities used to hold and process such User Data (e.g., use of key card access controls and security guard monitoring); and

1.3.1.2. use of data centers with 24/7 security protection, automatic fire detection and suppression, fully redundant power systems, and other reasonable environmental controls.

2. OPERATIONS MANAGEMENT AND NETWORK SECURITY

2.1. Gustave Connect establishes and maintains reasonable operations management and network security measures, including:

2.1.1. network segmentation based on the label or classification level of the information stored;

2.1.2. protection of servers and web applications using restrictive firewalls; and

2.1.3. regular review, testing, and installation of security updates and patches to servers.

3. CHANGE MANAGEMENT

3.1. Change and Release Management

3.1.1. Gustave Connect maintains a formal change and release management policy and procedure for software, system, and configuration changes. Such policies and procedures include:

3.1.1.1. a process for testing and approving promotion of changes into production; and

3.1.1.2. a process for performing security assessments of changes into production.

3.2. Secure Application Development

3.2.1. Gustave Connect follows secure application development policies, procedures, and standards that are aligned to industry-standard practices, such as the OWASP Top 10.

3.3. Development Training

3.3.1. Gustave Connect provides secure code development training based on role for secure application development, configuration, testing, and deployment.

4. DATA ENCRYPTION AND DELETION

4.1. Gustave Connect establishes and maintains reasonable data encryption and deletion practices, including:

4.1.1. encryption of User Data while at rest using industry best practice encryption standards and methods;

4.1.2. encryption of User Data while in transit using industry-standard encryption methods designed to encrypt communications between its server(s) and User browser(s);

4.1.3. use of cryptographic controls and approved algorithms for information protection within the service environment based on Gustave Connect's company policies and standards;

4.1.4. encryption of employee workstations with full disk encryption, strong passwords, and screen lockout; and

4.1.5. maintenance of policies and procedures regarding the deletion of User Data in accordance with applicable laws and ISM guidance (User Data is deleted upon User request and removed off Gustave Connect's cloud hosting provider servers).

5. SUB-PROCESSORS

Gustave Connect uses certain sub-processors to assist Gustave Connect in providing the Services. Prior to engaging any sub-processor who has access to, potentially will have access to, or processes User Data, Gustave Connect conducts an assessment of the security and privacy practices of the sub-processor to ensure they are commensurate with the level of data access the sub-processor will have and the scope of the services it will provide. Gustave Connect then enters into a written agreement with the sub-processor containing privacy, data protection, and data security obligations that ensure a level of protection appropriate to the sub-processor's processing activities. Gustave Connect performs annual reviews of its sub-processors to ensure that compliance and security standards are maintained and material changes to processes are reviewed.

6. SYSTEM MONITORING AND VULNERABILITY MANAGEMENT

6.1. Gustave Connect regularly monitors its production environment for unauthorized intrusions, vulnerabilities, and the like. Gustave Connect's system monitoring measures include the following:

6.1.1. use of intrusion detection methods to prevent and identify potential security attacks from users outside the boundaries of the system;

6.1.2. performance of automated application and infrastructure vulnerability scans to identify vulnerabilities, classification of vulnerabilities using industry standards, and remediation of vulnerabilities based on severity level;

6.1.3. annual third-party penetration testing (an executive summary can be provided upon request);

6.1.4. annual risk assessments and continuous monitoring of Gustave Connect's risk register;

6.1.5. periodic third-party security audits;

6.1.6. monitoring, logging, and reporting on critical or suspicious activities with regard to network devices, including retention of logs for forensic-related analysis, maintenance of audit logs that record and examine activity within Gustave Connect's production environment, back-up of logs in real-time, and implementation of controls to prevent modification or tampering of logs;

6.1.7. operation of a "bug bounty" program to identify potential security vulnerabilities; and

6.1.8. deployment of anti-virus and malware tools to detect and remediate harmful code or programs that can negatively impact the Services.

7. PERSONNEL CONTROLS

7.1. Gustave Connect uses reasonable efforts to ensure the continued reliability of Gustave Connect employees who have access to User Data by implementing the following measures:

7.1.1. conducting background checks, subject to applicable laws, on all employees who may access User Data;

7.1.2. requiring employees to complete new-hire security training and acknowledge Gustave Connect's information security policies, including but not limited to Gustave Connect's Code of Conduct and Acceptable Use of Technology Resources Policy, upon hire;

Data Processing Addendum

7.1.3. requiring employees to complete annual privacy and security training covering topics that address their obligations to protect User Data as well as privacy and security best practices;

7.1.4. instructing employees to report potential personal data breaches to the Security team; and

7.1.5. imposing discipline for material violations of Gustave Connect's information security policies.

8. BACKUPS, BUSINESS CONTINUITY, AND DISASTER RECOVERY

8.1. Backups

8.1.1. Gustave Connect maintains a policy and procedure for performing backups of User Data.

8.2. Business Continuity Program

8.2.1. Gustave Connect maintains a reasonable business continuity program, including a disaster recovery plan, designed to minimize disruption to the Services. The plans are tested annually and the process is amended, as needed.

9. AUDIT REVIEW

Upon User's written request (email to suffice), Gustave Connect will provide to User for review a copy of Gustave Connect's most recent annual audit results.