4me DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**Addendum**") is made and entered into by and between 4me, Inc., a Delaware corporation ("**4me**") and the customer specified in the table below ("**Customer**").

4me, Inc.	**Customer:**
Signature:	Signature:
Name:	Name:
Title:	Title:
Date signed:	Date signed:
Address: 555 Bryant Street #156 Palo Alto, California, 94301 U.S.A.	Address:

This Addendum supplements the 4me Customer Agreement available at https://www.4me.com/agreement, as updated from time to time between Customer and 4me, or other agreement between Customer and 4me governing Customer's use of the Services (the "**Agreement**"). Unless otherwise defined in this Addendum or in the Agreement, all capitalised terms used in this Addendum will have the meaning given to them in Section 19 (Definitions) of this Addendum.

1. Data Processing.

1.1. Scope and Roles. This Addendum applies when Customer Personal Data is processed by 4me. In this context, 4me will act as "processor" to Customer who acts as "controller" with respect to Customer Personal Data (as each term is defined in the GDPR).

1.2. Customer Controls. The Services provide Customer with a number of controls, including security features and functionalities, that Customer may use to access, rectify, erase or restrict processing of Customer Personal Data. Customer may use these controls as technical and organizational measures to assist it in connection with its obligations under data protection legislation including its obligations relating to responding to requests from data subject.

1.3. Details of Data Processing.

i. **Subject Matter.** The subject matter of the data processing under this Addendum is the Customer Personal Data.

ii. **Duration.** As between Customer and 4me, the duration of the data processing under this Addendum is determined by Customer. In general processing is happening as long as the customer is actively using the system.

iii. **Purpose.** The purpose of the data processing under the Addendum is the provision of the Services (as described in the 4me Customer Agreement available at https://www.4me.com/agreement) to Customer; as initiated by Customer.

iv. **Nature of the Processing.** Storage and other processing necessary to provide, maintain and improve the Services (as described in the 4me Customer Agreement available at https://www.4me.com/agreement) provided to Customer; as initiated by Customer.

v. **Categories of Data.** The Customer Personal Data uploaded to the Services in Customer's 4me accounts which may include, but not limited to, name and contact information.

vi. **Categories of Data Subjects.** The data subjects may include Customer's employees and contractors, customers, partners, suppliers, end users, and any person who uploads data via the Services, including individuals collaborating and communicating with end users.

1.4. Compliance with Laws. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this Addendum, including the GDPR.

1.5. Access or Use. 4me will not access or use Customer Data, except as necessary to maintain or provide the Services, or as defined in Section 3.

2. Customer Instructions. 4me will process Customer Data only in accordance with Customer's instructions. The parties agree that this Addendum with Appendixes is Customer's complete and final documented instruction to 4me in relation to Customer Data. Additional instructions outside the scope of this Addendum (if any) require prior written agreement between 4me and Customer, including agreement on any additional fees payable by Customer to 4me for carrying out such instructions. Customer is entitled to terminate this Addendum and the Agreement if 4me declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this Addendum. Customer shall ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Customer Data.

3. Confidentiality of Customer Data. 4me will not disclose Customer Data to any government or any other third party, except as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). In the event 4me receives an order from any third party for compelled disclosure of any personal data that has been transferred, 4me shall:
(a) use every reasonable effort to redirect the third party to request data directly from Data Controller;
(b) promptly notify Data Controller, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Data Controller, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Data Controller as soon as practicable; and
(c) use all reasonable efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union, applicable Member State law or Customer's local law.
For the purpose of this section, reasonable efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

4. Confidentiality Obligations of 4me Staff. 4me restricts its staff from processing Customer Data without authorization by 4me as described in the Security Measures. 4me imposes appropriate contractual obligations upon its staff, including relevant obligations regarding confidentiality, data protection and data security.

5. Subprocessing.

5.1. Authorized Subprocessors. Customer agrees that 4me may use subprocessors to fulfil its contractual obligations under this Addendum or to provide certain services on its behalf, such as providing support services. The 4me website lists at https://www.4me.com/subprocessors/ the subprocessors that are currently engaged by 4me to carry out specific processing activities on behalf of Customer. At least thirty (30) days before we authorize and permit any new Subprocessor to access any Customer Data, 4me will proactively inform customers. Customer can object to a new subprocessor by notifying 4me promptly in writing within thirty (30) business days after the announcement to engage the new subprocessor. Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new subprocessor, as permitted in the preceding sentence, 4me will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid processing of personal data by the objected-to new subprocessor without unreasonably burdening Customer. If 4me is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate without penalty the applicable Order Form(s) with respect only to those Services which cannot be provided by 4me without the use of the objected-to new subprocessor by providing written notice to 4me. 4me will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer. Except as set forth in this Section, or as Customer may otherwise authorize, 4me will not permit any subprocessor to carry out specific processing activities on behalf of Customer.

5.2. Subprocessor Obligations. Where 4me authorizes any subprocessor as described in Section 5.1:

i. 4me will restrict the access of subprocessor to Customer Data only to what is necessary to maintain the Services or to provide the Services to Customer and any End Users in accordance with the Documentation, 4me will prohibit the subprocessor from accessing Customer Data for any other purpose;

ii. 4me will enter into a written agreement with the subprocessor and, to the extent that the subprocessor is performing the same data processing services that are being provided by 4me under this Addendum, 4me will impose on the subprocessor the same contractual obligations that 4me has under this Addendum; and

iii. 4me will remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of the subprocessor that cause 4me to breach any of 4me's obligations under this Addendum.

6. Data Subject Rights. 4me shall assist the Customer, taking into account the nature of the processing and the information available to it, in complying with the obligations set out in Articles 32 to 36 GDPR. 4me offers Customer certain controls as described in Section 1.2 (Customer Controls) and Section 8.3 (Customer Security Controls) that Customer may elect to use to comply with its obligations towards data subjects.

6.1. Access, Rectification, Erase, Restrict, Portability. 4me will, in a manner consistent with the functionality of the Services, enable Customer to access, rectify, erase and restrict processing of Customer Personal Data, including via the erasure functionality provided by 4me as described in Section 7.1 (Erasure During Term), and to export Customer Data.

6.2. Data Subject Requests.

i. Customer's Responsibility for Requests. When 4me receives any request from a data subject in relation to Customer Personal Data, 4me will advise the data subject to submit his/her request to Customer, and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

ii. 4me Assistance. Customer agrees that (taking into account the nature of the processing of Customer Personal Data) 4me will assist Customer in fulfilling any obligation to respond to requests by data subjects, including, if applicable, Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by:

(a) providing the Customer Security Controls in accordance with Section 8.3 (Customer Security Controls)

(b) complying with the commitments set out in Section 6.1 (Access, Rectification, Erase, Restrict, Portability) and Section 6.2.i. (Customer's Responsibility for Requests).

Should a data subject contact 4me with regards to correction or deletion of its personal data, 4me will use commercially reasonable efforts to forward such requests to Customer without delay.

7. Data Erasure.

7.1. Erasure During Term. 4me will enable Customer and/or End Users to erase Customer Data during the applicable Term in a manner consistent with the functionality of the Services. If Customer or an End User uses the Services to erase any Customer Data during the applicable Term and the Customer Data cannot be recovered by Customer or an End User, this use will constitute an instruction to 4me to erase the relevant Customer Data from 4me's systems in accordance with applicable law. 4me will comply with this instruction as soon as reasonably practicable and within a maximum period of 30 days, unless applicable law requires storage or there are any contractual retention obligations to the contrary. 4me will inform the Customer when the data erasure will be completed.

7.2. Erasure on Term Expiry. Subject to Section 7.3 (Deferred Erasure Instruction), on expiry of the applicable Term Customer instructs 4me to erase all Customer Data (including existing copies) from 4me's systems in accordance with applicable law. 4me will comply with this instruction as soon as reasonably practicable and within a maximum period of 30 days after the account is settled, unless applicable law requires storage or there are any contractual retention obligations to the contrary. Without prejudice to Section 6.1 (Access, Rectification, Erase, Restrict, Portability), Customer acknowledges and agrees that Customer will be

responsible for exporting, before the applicable Term expires, any Customer Data it wishes to retain afterwards. 4me will inform the Customer when the data erasure will be completed.

7.3. Deferred Erasure Instruction. To the extent any Customer Data covered by the erasure instruction described in Section 7.2 (Erasure on Term Expiry) is also processed, when the applicable Term under Section 7.2 expires, in relation to an Agreement with a continuing Term, such erasure instruction will only take effect with respect to such Customer Data when the continuing Term expires. For clarity, this Addendum will continue to apply to such Customer Data until its erasure by 4me.

8. Security Measures, Compliance and Controls.

8.1. 4me Security Measures. 4me shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality, integrity and availability of Customer Data, as set forth in the 4me Security Measures. 4me regularly monitors compliance with these measures. 4me may update or modify the Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

8.2. Security Compliance by 4me Staff. 4me will take appropriate steps to ensure compliance with the Security Measures by its staff, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3. Customer Security Controls. 4me provides Customer with information about securing, accessing and using Customer Data, and makes available a number of security controls that Customer may elect to use. Customer is responsible for (a) properly configuring the Services, (b) using the controls available in connection with the Services (including the security controls) to ensure the ongoing confidentiality and integrity of Customer Data, and (c) taking such steps as Customer considers adequate to maintain appropriate security, protection, and erasure of Customer Data, which includes measures to control access rights to Customer Data.

9. Security Incident Response.

9.1. Incident Notification. If 4me becomes aware of a Security Incident, 4me will without undue delay: (a) notify Customer of the Security Incident; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. The notification shall include information about:
(a) the time and nature of the incident;
(b) the time of discovery;
(c) the data subjects and affected Controller Data, including an estimate of the number of affected data subjects and Controller Data;
(d) likely consequences of the data security incident and/or personal data breach;
(e) measures already adopted or proposed by the Processor to address or mitigate its possible adverse effects, where applicable.

9.2. No Assessment of Customer Data by 4me. 4me will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident(s).

9.3. Unsuccessful Security Incidents. Customer agrees that 4me assesses whether the personal data processed for the Customer is affected by a security incident. If not, this Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorised access to Customer Data or to any of 4me's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful access attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents.

9.4. No Acknowledgement of Fault by 4me. 4me's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by 4me of any fault or liability of 4me with respect to the Security Incident.

9.5. Communication. Notifications of Security Incidents, if any, will be delivered to Customer's EU representative and/or Customer's data protection officer by any means 4me selects, including via email. It is Customer's sole responsibility to ensure Customer's 4me account owner maintains accurate contact information within the 4me Settings console section "Legal & Compliance", and secure transmission at all times.

9.6. Privacy Impact Assessment and Prior Consultation. The information made available by 4me under this Section 9 is intended to assist Customer in complying with Customer's obligations under the GDPR with respect to data protection impact assessments and prior consultation.

10. Certifications and Audits.

10.1. 4me Audits.

i. 4me engages credentialed external auditors to verify the adequacy of its security measures. This audit: (a) will be performed at least annually; (b) will be performed according to industry standards; (c) will be performed by independent third-party security professionals at 4me's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be 4me's Confidential Information. If Customer's Agreement does not include a provision protecting 4me Confidential Information, then Reports will be made available to Customer subject to a mutually agreed upon non-disclosure agreement covering the Report (an "NDA").

ii. 4me engages independent entities to conduct regular application-level and infrastructure-level penetration tests. Results of these tests are shared with 4me management. 4me's security team reviews and prioritizes the reported findings and tracks them to resolution. Customers wishing to conduct their own penetration test of the Services may request to do so and should contact their account representative to obtain permission from both 4me and 4me's hosting provider.

iii. 4me's SaaS platform is compliant with the requirements of SOC 2 Type 2 for information security, availability and privacy, as well as ISO 27001:2013 and ISO 27018:2019. To evaluate and help ensure the continued effectiveness of the security measures, 4me will update the SOC 2 report at least once every 12 months and will undergo yearly surveillance audits and a recertification audit after three years for the ISO certifications .

10.2. Audit Reports. At Customer's written request, 4me will provide Customer with a confidential Report so that Customer can reasonably verify 4me's compliance with its obligations under this Addendum. The Report will constitute 4me's Confidential Information under the confidentiality provisions of the Agreement or the NDA, as applicable.

10.3. Independent Determination. Customer is responsible for reviewing the information made available by 4me relating to data security and making an independent determination as to whether the Services meets Customer's requirements and legal obligations as well as Customer's obligations under this Addendum.

10.4. Regulator Audits. 4me grants Regulators the unrestricted rights of inspection and auditing related to the Services (hereinafter "Audit Rights") to enable them to monitor the Services and to ensure compliance with all applicable regulatory and contractual requirements. This Audit Right comprises, but is not limited to, the direct right to examine the Services, including the right to conduct an on-premise assessment and examination at 4me's offices and/or the right to copy relevant documents for this purpose. For this purpose, any person or entity exercising an internal or external audit function at 4me is released from any obligation of confidentiality and/or professional secrecy with respect to Customer to the extent required to comply with these Audit Rights.

10.5. Customer Audits. 4me also grants Audit Rights described in 10.4 of this Addendum to Customer and any other person or legal entity appointed by each of them with respect to the Services, but only to the extent necessary to comply with laws and regulatory requirements of any applicable jurisdiction. Customer may exercise this Audit Right annually. If 4me declines to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this Addendum and the Agreement.

11. Transfers of Personal Data.

11.1. Storage Locations. All Customer Data in accounts ending with *.4me.com and *.4me.qa is stored and processed within the European Economic Area (EEA) - 4me will not transfer Customer Data from the EEA except as described in Section 3 (Confidentiality of Customer Data) of the Agreement. All Customer Data in accounts ending with *.au.4me.com and *.au.4me.qa is stored and processed in Australia - 4me will not transfer Customer Data from Australia except as described in Section 3 (Confidentiality of Customer Data) of the Agreement. All Customer Data in accounts ending with *.uk.4me.com and *.uk.4me.qa is stored and processed in the United Kingdom - 4me will not transfer Customer Data from the United Kingdom except as described in Section 3 (Confidentiality of Customer Data) of the Agreement.

12. Data Protection Team and Processing Records.

12.1. Data Protection Team. 4me's Data Protection Team can be contacted by Customer's 4me account administrators via privacy@4me.com and/or by Customer by providing a notice to 4me as described in the applicable Agreement.

12.2. Processing Records. Customer acknowledges that 4me is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which 4me is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer Personal Data, Customer will, where requested, provide such information to 4me in the "Legal & Compliance" section that is available in the Settings console of the Services when logged in as the owner of Customer's 4me accounts, or other means provided by 4me, and will use the Settings console or such other means to ensure that all information provided is kept accurate and up-to-date.

13. Limitations of Liability. The liability of each party under this Addendum shall be subject to the exclusions and limitations of liability set out in the Agreement. Customer agrees that any regulatory penalties incurred by 4me in relation to the Customer Personal Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this Addendum and the GDPR, or non-EU data protection legislation, shall count towards and reduce 4me's liability under the Agreement. Liability is according to Art. 82 GDPR.

14. Duties to Inform. Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by 4me, 4me will inform Customer without undue delay. 4me will, without undue delay, notify all relevant parties in such action (e.g. creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.

15. Nondisclosure. Customer agrees that the details of this Addendum are not publicly known and constitute 4me's Confidential Information under the confidentiality provisions of the Agreement or NDA. If the Agreement does not include a confidentiality provision protecting 4me Confidential Information and Customer and 4me or its Affiliates do not have an NDA in place covering this Addendum, then Customer will not disclose the contents of this Addendum to any third party except as required by law.

16. Entire Agreement; Conflict. This Addendum supersedes and replaces all prior or contemporaneous representations, understandings, agreements, or communications between Customer and 4me, whether written or verbal, regarding the subject matter of this Addendum, including any data processing addenda entered into between 4me, Inc. and Customer containing terms and conditions in respect of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Except as amended by this Addendum, the Agreement will remain in full force and effect.

17. Effective Date. This Addendum shall become effective between the respective Data Controller and Data Processor when these two parties are bound by an effective Customer Agreement and when both aforementioned Parties have signed this Addendum. This Addendum shall be executed in counterparts, each of which shall be deemed an original, but all of which together shall be deemed to be one and the same agreement. A signed copy of this Addendum delivered by e-mail as a PDF shall be deemed to have the same legal effect as delivery of an original signed copy of this Addendum.

18. Termination of the Addendum. This Addendum shall continue in force until the termination of the Agreement.

19. Definitions. Unless otherwise defined in the Agreement, all capitalised terms used in this Addendum will have the meanings given to them below:

"**4me Infrastructure**" means data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within 4me's control and are used to provide the Services.

"**4me Security Measures**" means the security measures attached to the Agreement, or if none are attached to the Agreement, attached to this Addendum as Annex 1.

"Customer Data" means data that is uploaded to the Services in Customer's 4me accounts.

"Customer Personal Data" means the "personal data" (as defined in the GDPR) contained within the Customer Data.

"**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**EEA**" means the European Economic Area.

"**processing**" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

"**Security Incident**" means a breach of security of the 4me Security Measures leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data. "Security Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful access attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"Services" means any product or service provided by 4me to Customer pursuant to the Agreement..

"SOC 2 Report" means a confidential Service Organization Control (SOC) 2 Report (or a comparable report) on 4me's systems examining logical security controls, physical security controls, and privacy controls, as produced by 4me's third-party auditor in relation to the audited Services.

"**Term**" means the period from this Addendum Effective Date until the end of 4me's provision of the Services under the applicable Agreement, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which 4me may continue providing the Services for transitional purposes.

ANNEX 1

4me Security Measures

4me will implement and maintain the Security Measures set out in this Annex 1 to the Data Processing Addendum. 4me may update or modify the Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

1. **Information Security Program.** 4me will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the 4me Information Security Policy, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the 4me Infrastructure, and (c) minimise security risks, including through risk assessment and regular testing. 4me will designate one or more staff to coordinate and be accountable for the information security program. The information security program will include the following measures:

   1.1. Data Centers. 4me relies solely on the secure cloud infrastructure provided by its subprocessor AWS to store and process all Customer Data logically across multiple availability zones within the EEA region or the Australian region, protecting the Services from loss of connectivity, power infrastructure and other common location-specific failures.

   1.2. Physical Security. All data centers that run the Services are secured and monitored 24/7 and physical access to the data centers is strictly limited to select AWS staff who have a legitimate business need for such access privileges. No staff of 4me has, nor will be permitted to have, physical access to the data centers. This measure survives the end of the contract a staff member has with 4me.

   1.3. Infrastructure Security. The 4me Infrastructure will be electronically accessible to 4me staff, contractors and any other person as necessary to provide the Services. 4me will maintain access controls and policies to manage what access is allowed to the 4me Infrastructure from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. 4me will maintain corrective action and incident response plans to respond to potential security threats.

   1.4. Instance Security. 4me takes all necessary precautions to ensure that every layer involved in data transfer is secured by best-of-breed technologies. Services are based on a security-oriented bare minimal, lightweight operating system, preventing the exploitation of entire classes of zero-day and other vulnerabilities.

   1.5. Customer Data Security. The Services support the latest recommended secure cipher suites and protocols to encrypt all data traffic in transit. All Customer Data is encrypted at rest – including, but not limited to: databases, search indexes, files storage, memory caches, log data, backups, and all disks.

   1.6. Access Security.

      i. Infrastructure Security Staff. 4me has, and maintains, a security policy for its staff, and requires security training as part of the training package for its staff. 4me's infrastructure security staff are responsible for the ongoing monitoring of 4me's security infrastructure, the review of the Services, and responding to security incidents.

      ii. Customer Access. In addition to the security measures 4me employs for its processes, systems and staff, 4me provides administrators of 4me accounts capabilities to enable their own users to protect their Customer Data. This includes controls such as role-based access, single sign on, SCIM provisioning, multi-factor authentication, password policies, visibility into audit trails and access logs, data retention settings, and capabilities to rectify, erase and restrict processing of Customer Personal Data.

      iii. Internal Data Access. 4me's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process Customer Data. 4me aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer Data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. 4me employs a centralized access management system to control staff access to production systems, and only provides access to a limited number of authorized staff. All access

mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. 4me requires the use of unique user IDs, strong passwords, two-factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized staff's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with 4me's internal data access policies and training. Approvals are managed by 4me that maintain audit trails of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication, password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength.

1.7. Personnel Security. 4me staff members are required to conduct themselves in a manner consistent with the 4me's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. 4me conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations. Staff members are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, 4me's security and privacy policies. Staff members are provided with security training annually and privacy training bi-annually. 4me staff members will not process Customer Data without authorization.

1.8. Subprocessor Security. Before using a Subprocessor, 4me conducts an audit of the security and privacy practices of the Subprocessor to ensure the Subprocessor provides a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once 4me has assessed the risks presented by the Subprocessor, then subject always to the requirements set out in Section 5 (Subprocessing) of this Data Processing Addendum, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

2. Additional measures. Following the decision of European Court of Justice No. 311/18 (Schrems II) 4me certifies that (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (3) that national law or government policy does not require the Processor to create or maintain back doors or to facilitate access to personal data or systems or for the Processor to be in possession or to hand over the encryption key.

3. Continued Evaluation. 4me will conduct periodic reviews of the security of its 4me Infrastructure and adequacy of its information security program as measured against industry security standards and its policies and procedures. 4me will continually evaluate the security of its 4me Infrastructure and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.