4me DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**Addendum**") is effective as of the date of the last signature below (the "**Addendum Effective Date**") and 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 may act either as "controller" or "processor" 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 the GDPR and non-EU 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.

iii. **Purpose.** The purpose of the data processing under the Addendum is the provision of the Services to Customer; as initiated by Customer.

iv. **Nature of the Processing.** Storage and other processing necessary to provide, maintain and improve the Services provided to Customer.

v. **Categories of Data.** The Customer Personal Data uploaded to the Services in Customer's 4me accounts.

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 necessary to comply with the law or binding order of a government body.

2. **Customer Instructions.** 4me will process Customer Data only in accordance with Customer's instructions. The parties agree that this Addendum 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 law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends 4me a demand for Customer Data, 4me will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, 4me may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then 4me will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless 4me is legally prohibited from doing so.

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 update this page to 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. Taking into account the nature of the Services, 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.

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 180 days, unless applicable law requires storage.

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 180 days, unless applicable law requires storage. 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.

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.

9.2. 4me Assistance. To assist Customer in relation to any personal data breach notifications Customer is required to make under the GDPR, 4me will include in the notification under section 9.1 (a) such information about the Security Incident as 4me is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to 4me, and any restrictions on disclosing the information, such as confidentiality.

9.3. 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).

9.4. Unsuccessful Security Incidents. Customer agrees that an unsuccessful 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.

9.5. 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.

9.6. 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.

9.7. 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 is compliant with the requirements of SOC 2 Type 1 for information security, availability and privacy and seeks compliance with the requirements of SOC 2 Type 2 and ISO 27001:2013. 4me will update the SOC 2 report at least once every 12 months to evaluate and help ensure the continued effectiveness of the Security Measures.

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. Customer Audits. Customer agrees to exercise any right it may have to conduct an audit or inspection, by instructing 4me to carry out the audit described in Section 10.1. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending 4me written notice as provided for in the Agreement. 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 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.

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.

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. If there is a conflict between any other agreement between the parties including the Agreement and this Addendum, the terms of this Addendum will control.

17. **Effective Date.** This Addendum will be effective as of the date of the last signature, and only if the information at the top of this Addendum is completed, signed and send by email to dpa@4me.com, and receipt of the validly completed Addendum has been confirmed by 4me.

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, 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. 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.

ANNEX 2

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as "Customer" in the DPA
(the "**data exporter**")

and

4me, Inc.
555 Bryant Street #156
Palo Alto, California, 94301
USA

(the "**data importer"**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in 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;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and

Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and received no objection;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior information of the data exporter.
   Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is the entity identified as “Customer” in the DPA

Data importer

The data importer is the entity identified as “4me, Inc.” in the DPA.

Data subjects

Data subjects are defined in Section 1.3 of the DPA.

Categories of data

The personal data is defined in Section 1.3 of the DPA.

Processing operations

The personal data transferred will be subject to the data processing activities defined in Section 1.3 of the DPA.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organisational security measures implemented by the data importer are as described in the DPA.