# 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:<br>555 Bryant Street #156<br>Palo Alto, California, 94301<br>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 capitalized 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" or "operator" to Customer who acts as "controller" or "responsible party" with respect to Customer Personal Data (see **19. Definitions**).

**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 as well as juristic personal 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 data processing laws.

**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. **Law Enforcement.** In the event 4me receives an order from a law enforcement agency for compelled disclosure of any Customer Personal Data, 4me shall use reasonable effort to:

(a) redirect the law enforcement agency directly to the Data Controller;
(b) promptly notify the Data Controller;
(c) 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.

Reasonable effort is used to the extent 4me is legally permitted to.

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

5. **Subprocessing.**

**5.1. Authorized Subprocessors.** Customer agrees that 4me may use subprocessors to fulfill 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 (see **19. Definitions**), by:

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

  - **(b)** complying with the commitments for rectification, erase, restrict, portability) and supporting 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 impacting Customer's operation or unauthorized access to Customer data, 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 unauthorized 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 unauthorized 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, as well as other security and compliance related communication mentioned in this Data Processing Addendum, will be delivered to Customer's EU representative (if applicable) and/or Customer's data protection/security 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 applicable data protection law with respect to data protection impact assessments and prior consultation. 4me will provide Customer with additional documentation for Customer's compliance obligations if deemed necessary by Customer and if distribution is permitted for the requested documentation.

**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.

**i.** 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. 4me will notify Customer if there is any change in its audit strategy or if a significant finding/deviation during an audit will prevent 4me from continuing the above mentioned compliance strategy and therefore maintaining the mentioned 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 is stored and processed either within the European Economic Area (EEA), the United Kingdom, Switzerland, Australia and the United States of America depending on the Customer's data processing location decision.

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 applicable data processing laws 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, 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. In order to obtain an adequate level of protection of privacy and the rights and freedoms of persons whose data an European Customer entrusts for processing, the Parties agree to the Standard Contractual Clauses, which are included in Annex 2 to the Addendum. If there is a conflict between any other agreement between the parties including the Agreement and this Addendum, the terms of this Addendum including the Standard Contractual Clauses will control. In case there is a conflict between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses will control.

17. **Effective Date.** This Addendum shall become effective between the respective Controller and 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 capitalized 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.

**"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

**"Customer Data"** means data that is uploaded to the Services in Customer's 4me accounts and may include Customer Personal Data.

**"Customer Personal Data"** means the "personal data" (as defined in the GDPR and other data processing laws) contained within the Customer Data.

**"Data Subject's Rights"** according to Chapter III of the GDPR and section 5 of POPIA.

"**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.

**"Operator"** means a person or company who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party according to POPIA.

**"POPIA"** means The Protection of Personal Information Act, 2013 (Act 4 of 2013) of South Africa with regard to processing of personal data, including juristic personal information.

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

**"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**"Responsible Party"** is the public or private body or any other person, which alone or in conjunction with others, determines the purpose of and means for processing personal information according to POPIA

"**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) minimize 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 on the secure cloud infrastructure provided by its subprocessor AWS to store and process all Customer Data logically across multiple availability zones within the Customer selected 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.

**ANNEX 2 (where applicable)**

# STANDARD CONTRACTUAL CLAUSES

# SECTION I

## *Clause 1*

## Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

b. The Parties:

   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

   have agreed to these standard contractual clauses (hereinafter: "Clauses").

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

## *Clause 2*

## Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of

Regulation (EU) 2016/679.

### *Clause 3*

### Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
    i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
    ii. Clause 8.1 b., 8.9 a., c., d. and e.;
    iii. Clause 9 a., c., d. and e.;
    iv. Clause 12 a., d. and f.;
    v. Clause 13;
    vi. Clause 15.1 c., d. and e.;
    vii. Clause 16 e.;
    viii. Clause 18 a. and b.;
b. Paragraph a. is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### *Clause 4*

### Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### *Clause 5*

### Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

### *Clause 6*

### Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

### *Clause 7 - Optional*

### Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## SECTION II – OBLIGATIONS OF THE PARTIES

### *Clause 8*

### Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

**MODULE TWO: Transfer controller to processor**

**8.1 Instructions**

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU)

2016/679.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

**8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14 e. to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14 a..

**8.6 Security of processing**

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more

information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offenses (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

**8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.9 Documentation and compliance**

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
e. The Parties shall make the information referred to in paragraphs b. and c., including the results of any audits, available to the competent supervisory authority on request.

## *Clause 9*

## Use of sub-processors

**MODULE TWO: Transfer controller to processor**

a. OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
c. The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfill its obligations under that contract.
e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

## *Clause 10*

## Data subject rights

**MODULE TWO: Transfer controller to processor**

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.
b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
c. In fulfilling its obligations under paragraphs a. and b., the data importer shall comply with the instructions from the data exporter.

## *Clause 11*

## Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

**MODULE TWO: Transfer controller to processor**

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
    i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    ii. refer the dispute to the competent courts within the meaning of Clause 18.
d. The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## *Clause 12*

## Liability

**MODULE TWO: Transfer controller to processor**

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
c. Notwithstanding paragraph b., the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
d. The Parties agree that if the data exporter is held liable under paragraph c. for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
f. The Parties agree that if one Party is held liable under paragraph e., it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

## *Clause 13*

## Supervision

**MODULE TWO: Transfer controller to processor**

a. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

# SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

## *Clause 14*

## Local laws and practices affecting compliance with the Clauses

**MODULE TWO: Transfer controller to processor**

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph a., they have taken due account in particular of the following elements:

   i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

   ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[12];

   iii. any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph b., it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph b. and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph a., including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph a..

f. Following a notification pursuant to paragraph e., or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16d. and e. shall apply.

## *Clause 15*

## Obligations of the data importer in case of access by public authorities

**MODULE TWO: Transfer controller to processor**

**15.1 Notification**

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
    i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
    ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs a. to c. for the duration of the contract and make it available to the competent supervisory authority on request.
e. Paragraphs a. to c. are without prejudice to the obligation of the data importer pursuant to Clause 14e. and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14e..
b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

# SECTION IV – FINAL PROVISIONS

## *Clause 16*

## Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14f..
c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
    i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph b. and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
    ii. the data importer is in substantial or persistent breach of these Clauses; or
    iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph c. shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

## *Clause 17*

## Governing law

**MODULE TWO: Transfer controller to processor**

OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of (*specify Member State*).

## *Clause 18*

## Choice of forum and jurisdiction

**MODULE TWO: Transfer controller to processor**

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
b. The Parties agree that those shall be the courts of (*specify Member State*).

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

---

1 Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

2 This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

3 The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

4 The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

5 See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

6 The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

7 This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offenses.

8 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

9 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

10 That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

11 The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

12 As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

# APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can [be] achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

# ANNEX I

**A. LIST OF PARTIES**

**MODULE TWO: Transfer controller to processor**

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name:
   Address:

   Contact person's name, position and contact details:

   Activities relevant to the data transferred under these Clauses:

   Signature and date:

   Role (controller/processor): controller

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: 4me, Inc.
   Address: 555 Bryant Street #156
   Palo Alto, California, 94301
   U.S.A.
   Contact person's name, position and contact details: Laurens Pit, DPO, dpo@4me.com

   Activities relevant to the data transferred under these Clauses: 4me Service management Platform development, management and support

   Signature and date:

   Role (controller/processor): processor

**B. DESCRIPTION OF TRANSFER**

**MODULE TWO: Transfer controller to processor**

*Categories of data subjects whose personal data is transferred*

Employees, Customers, Suppliers, Consultants, Contractors

*Categories of personal data transferred*

Non-sensitive data e.g. name, email address, phone number

*Sensitive data transferred (if applicable) 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.*

The contents of the Personal Data are varied and under the data exporter's control, but may, from time to time, include sensitive data under the relevant Data Protection Laws. Data exporter acknowledges and agrees that Processor provides facilities for special handling of sensitive data, including data retention periods, pseudonymization, account restrictions and data masking depending on the function used.

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

In general the data is hosted and processed in Europe and will not be transmitted further. There is infrequent transfer of data during (customer initiated) support requests where customer data in this support request can be accessed by support specialists outside Europe due to 24/7 support.

*Nature of the processing*

Storage and other processing necessary to provide, maintain and improve the Services provided to Customer; as initiated by Customer.

*Purpose(s) of the data transfer and further processing*

The purpose of the data processing is the provision of the Services to Customer; as initiated by Customer.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

The duration of the data processing is determined by Customer. In general processing is happening as long as the customer is actively using the system.

*For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing*

The subprocessors are facilitating the Virtual Private Cloud Infrastructure (data centers) and the business integration and automation service which are used by the Processor to provide the Service (including the 4me Workflow Automator Service).

**C. COMPETENT SUPERVISORY AUTHORITY**

**MODULE TWO: Transfer controller to processor**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

The competent supervisory authority in the Customer Member State (list see https://edpb.europa.eu/about-edpb/about-edpb/members_en)

## ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

**MODULE TWO: Transfer controller to processor**

EXPLANATORY NOTE:

The technical and organizational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

*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.*

- Measures of pseudonymisation and encryption of personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing
- Measures for user identification and authorisation
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which personal data are processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for certification/assurance of processes and products
- Measures for ensuring data minimisation
- Measures for ensuring data quality
- Measures for ensuring limited data retention

- Measures for ensuring accountability
- Measures for allowing data portability and ensuring erasure

*For transfers to (sub-)processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*

Amazon Web Services (AWS)

- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which personal data are processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for certification/assurance of processes and products

Workato

- Maintains an information security program which is approved by its management and regularly reviewed and updated accordingly.
- Restricts access to Personal Data to Authorized Individuals who provide authentication that uniquely identifies them.
- Restricts Authorized Individuals' rights to access or modify Personal Data based on business role and need.
- Reviews access and authorization rights for Authorized Individuals regularly. Access or authorization rights are withdrawn or modified, as appropriate, promptly upon termination or change of role for such Authorized Individuals.
- Ensures that physical access to systems storing or Processing Personal Data is appropriately secured and monitored.
- Encrypts Personal Data both at rest and in transit, using industry standard protocols and encryption algorithms.
- Has implemented and maintains secure coding and development standards, incorporating security and privacy considerations.
- Ensures that its personnel receive regular security and privacy training so that they are aware of their roles and

responsibilities with regard to the treatment and protection of Personal Data.

- Segregates internal systems storing or processing Personal Data from public networks.
- Has implemented anti-malware on systems that do or may Process Personal Data.
- Has implemented monitoring and alerting capabilities on its systems.
- Evaluates its systems for vulnerabilities and deploys required security updates on a schedule based on risk and severity.
- Regularly tests the security of its systems including an annual penetration test performed by a qualified third party.
- Evaluates the security and privacy practices of all Authorized Sub-Processors. All Authorized Sub- Processors are required to implement and maintain the same or substantially similar technical and organizational measures and assume the same responsibilities and obligations as those required of Processor under this DPA.
- Deploys redundant services and engages in practices including regular backups designed to provide continued availability and access to data despite disruptions to its infrastructure.
- Maintains an incident response plan and commits to providing required notifications in case of a confirmed Personal Data Breach without undue delay.
- Maintains systems and processes for complying with data privacy requirements including limited retention and processing of requests from Data Subjects.

## ANNEX III – LIST OF SUB-PROCESSORS

**MODULE TWO: Transfer controller to processor**

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorized the use of the following sub-processors:

1. Name: Amazon Web Services
   Address: 410 Terry Ave North
   Seattle, WA 98109-5210
   U.S.A.
   Attention: General Counsel

   Description of processing: Facilitating the Virtual Private Cloud Infrastructure (data centers) to enable the Processor to provide the Service.

2. Name: Workato, Inc.
   Address: 215 Castro Street, Suite 300
   Mountain View, CA 94041
   U.S.A.
   Attention: Chief Information Security Officer, privacy@workato.com

   Description of processing: Workato provides a flexible business integration and automation service which is used by the Processor to provide the 4me Workflow Automator Service.