# DATA PROCESSING AGREEMENT
## Version 1.1 – 05/2021

This Data Processing Agreement is made as of the Effective Date between MOSTLY AI Solutions MP GmbH, a limited liability company incorporated under the laws of Austria, registered with the Commercial Court of Vienna under the registration number 466390v and having its corporate address at 1010 Vienna, Hegelgasse 21/3, Austria ("**MOSTLY AI**" or "**Provider**") and the Customer which has accepted the terms and conditions of the MOSTLY AI Software License Agreement and/or Professional Services Agreement, available at https://www.mostly.ai/terms/ (collectively, the "**Agreement**"). By executing an Order Form incorporating the terms of this Data Processing Agreement, the Customer thereby expressly agrees to be bound by the terms hereof.

**IN CONSIDERATION OF the provisions contained in this Data Processing Agreement, the parties agree as follows:**

### 1. Definitions

1.1 In addition to the definitions set out in the Agreement, the following definitions shall apply for this Data Processing Agreement:

(a) The term **"Personal Data Breach**", as used herein, shall have the same meaning as "personal data breach" under Article 4(12) GDPR.

(b) The term "**Processing Service**" or "**Processing Services**", as used herein, shall mean the (processing) services rendered by the Processor under the Agreement.

(c) The term **"Processor"**, as used herein, shall refer to the Provider.

(d) The term **"Controller"**, as used herein, shall refer to the Customer.

(e) The term **"DPA"**, as used herein, shall refer to this Data Processing Agreement.

**(f)** The term **"Effective Date"**, as used herein, shall have the meaning ascribed to such term in the Order Form incorporating the terms of this DPA.

All terms not otherwise defined in this DPA or the Agreement shall have the meaning ascribed to such terms in the GDPR.

### 2. Duration, Subject-Matter, Nature and Purpose of the Processing

2.1 For the duration of the Agreement, the Processor may, in exceptional circumstances, on behalf of the Controller, process personal data for the purpose of remedying defects or providing maintenance and support services. The purpose of the processing is to enable the Customer the synthetization of Personal Data.

2.2 This DPA shall prevail in the event of inconsistencies between it and the Agreement or subsequent agreements entered into or purported to be entered into by the parties after the date of this DPA, except where explicitly agreed otherwise in writing.

### 3. Right to Instruction

3.1 Unless otherwise required by EU or Member State law to which the Processor is subject, the Processor shall process the personal data only on documented instructions from the Controller. This includes the transfer of personal data to a third country or an international organization. Unless otherwise agreed between the parties, the Controller may only issue instructions to the Processor using the user interface of the Service.

3.2 The Processor shall immediately inform the Controller if, without seeking internal or external legal advice, it considers that an instruction issued by the Controller violates the GDPR or other data protection provisions of the EU or a Member State in a way that is apparent to a layperson. The Processor shall not be obliged to seek legal advice in connection with the performance of this DPA and will not provide any such legal advice to the Controller.

3.3 If such notification is permissible, the Processor shall inform the Controller if it is obliged, under EU or Member State law, to process personal data contrary to or without the instructions of the Controller.

### 4. Confidentiality

The Processor shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

**5. Data Security**

5.1 The Processor takes all measures required under Article 32 GDPR. The Processor fulfills this obligation by implementing the measures set out in Exhibit 1.

5.2 The Processor shall inform the Controller of any Personal Data Breach, insofar as such breach concerns personal data processed by the Processor on behalf of the Controller and results in a risk to the rights and freedoms of natural persons. This information shall be provided without undue delay after the Processor becomes aware of such a breach.

5.3 The information provided to the Controller pursuant to Section 5.2 shall include the following, to the extent feasible under the circumstances:

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

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

c. the measures taken or proposed to be taken by the Processor to address the Personal Data Breach.

**6. Sub-Processing**

6.1 The Controller hereby authorizes the Processor to engage the entities listed in Exhibit 2 as a sub-processor.

6.2 The Processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors or sub-processors (hereinafter collectively "**Sub-Processors**"), thereby giving the Controller the opportunity to object to and prohibit such changes. If the Controller does not object within two weeks, the addition or replacement shall be deemed to have been approved.

6.3 If an objection is raised in accordance with Section 6.2, the Processor shall be entitled to terminate the Agreement as well as this DPA at any time, subject to giving two weeks' prior notice.

6.4 Where the Processor engages another Sub-Processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in this DPA shall be imposed on that Sub-Processor by means of a contract. This contract shall in particular provide sufficient guarantees by the Sub-Processor to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of applicable data protection law.

6.5 Subject to the limitations of liability set out in the Agreement, where a Sub-Processor fails to fulfil its data protection obligations, the Processor shall remain liable to the Controller for the performance of that Sub-Processor's obligations.

6.6 Notwithstanding Section 5, where

a. the Processor informs the Controller of the use of any Sub-Processors and includes or makes available upon request information on the contractual terms offered by such Sub-Processors, including the technical and organizational measures implemented by such Sub-Processors (**"Sub-Processing Terms"**), and

b. the Controller approves or is deemed to have approved such Sub-Processors pursuant to Sections 6.1 or 6.2,

these Sub-Processing Terms shall be considered to be in full compliance with the terms of this DPA, including Sections 5 and 6.

**7. Assistance**

7.1 The Processor shall assist the Controller by appropriate technical and organizational measures, insofar as this is feasible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights under applicable data protection law, including Chapter III of the GDPR.

7.2 The Processor may choose to fulfil its obligation under Section 7.1 by forwarding requests received from data subjects to the Controller.

7.3 Moreover, the Processor shall assist the Controller with ensuring compliance with the Controller's obligations under applicable data protection law, including Articles 32 to 36 of the GDPR. The Processor shall do so by (i) taking the measures set forth in Section 4 ("Confidentiality") and Section 5 ("Data Security") of this DPA; (ii) notifying the Controller of a Personal Data Breach pursuant to Section 5.2; and (iii) providing the information set forth in Exhibit 1 of this DPA.

**8. Return of Personal Data**

8.1 The Controller acknowledges that the Processor will delete Personal Data prior to the end of the provision of the Processing Services as set out in the Terms. Should any Personal Data remain at the end of the provision of the Processing Services, the Controller hereby instructs the Processor to delete such Personal Data.

**9. Audit**

9.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA.

9.2 The Processor shall allow for pre-notified inspections to be carried out during business hours by the Controller or an independent third party. Such inspections shall be carried out at reasonable intervals and in a manner that does not interfere with the business of the Processor. Costs arising from such audits shall be borne by the Controller. The Processor shall be entitled to reasonable remuneration for all services rendered in connection with its support of inspections.

9.3 The Processor may also fulfil its obligations under Section 9.2 by having an independent third party carry out an audit at least every three years and providing the summary audit report to the Controller. Moreover, as regards a particular Sub-Processor, the Processor may fulfill its obligations under Section 9.2 by exercising its audit rights as provided in the agreement concluded between the Processor and the Sub-Processor or providing the Controller with the audit reports received from the Sub-Processor.

**10. Limitation on Liability**

10.1 The parties' liability under this DPA shall be limited as set forth in the Agreement.

## EXHIBIT 1

## TECHNICAL AND ORGANIZATIONAL MEASURES FOR THE PROTECTION OF PERSONAL DATA

1) Preventive Security Measures - Measures to Prevent a Successful Attack

   a) Technical measures

      (i) Logical access control: Access rights are granted according to the “need-to-know” principle.

      (ii) Authentication: Personal data is accessible only after successful authentication.

      (iii) Password security: Passwords used for authentication consist of at least 8 characters, lower and upper case letters, numbers, and special characters. Passwords are stored encrypted only.

      (iv) Encryption on the transmission path: Personal data is encrypted if transmitted over the Internet, at least to the extent sensitive data is concerned.

      (v) Encryption at rest: Any Personal Data uploaded to the Service will be encrypted at rest.

      (vi) Encryption of mobile devices: Mobile devices and mobile data carriers are encrypted, at least in case of sensitive data being stored on these devices.

      (vii) Network security: A firewall is used that separates the internal network from the Internet and – to the extent feasible – blocks incoming malicious network traffic.

      (viii) Measures against malicious software: Anti-virus software is used on all PCs and laptops to the extent feasible. All incoming emails are automatically scanned for malicious software.

      (ix) Management of security vulnerabilities: To the extent feasible, the automatic installation of security updates is activated on all devices. Otherwise, relevant security updates will be installed within a reasonable time.

   b) Organizational measures

      (i) Clear responsibilities: Internal responsibilities for data security issues are defined.

      (ii) Confidentiality requirements of employees: Employees are obliged to maintain secrecy beyond the duration of their employment. Employees may only transfer personal data to third parties at the explicit instruction of a supervisor.

      (iii) Training and information activities: Employees are trained on data security issues (internally or externally) and adequately informed about data security issues (such as password security).

      (iv) Orderly termination of employment relationships: There is a process in place to deactivate all accounts within a reasonable time after the effectiveness of the termination of an employment relationship.

      (v) Management of computer hardware: Records are kept of the distribution of end devices to specific employees (e.g., PC, laptop, mobile phone).

      (vi) Input control: Control procedures are implemented to control the accuracy of personal data.

      (vii) No duplicates of user accounts: Each person should have their own user account. The sharing of user accounts is prohibited.

      (viii) Limited use of administrative accounts: User accounts with administrative rights are only used in exceptional cases. IT systems are normally used without administrative rights.

      (ix) Selection of service providers: When selecting service providers, the data security level offered by the service provider is taken into account. Service providers that are considered a processor are only used after execution of a DPA.

      (x) Secure data disposal: Paper documents containing personal data are generally shredded or handed over to an external service provider for secure destruction. Storage media are completely overwritten or physically destroyed or otherwise disposed of in a secure manner.

c) Physical measures

(i) Physical access control: Access to business premises where personal data is processed is only permitted for non-employees if accompanied by a company employee or after authorization by a company employee.

(ii) Measures against burglary: Access to business premises where personal data is processed is equipped with adequate burglary protection (e.g., with security doors).

(iii) Special protection of computer hardware: Access to premises where computer servers are located is protected by special security measures (for example, by additional locks and/or CCTV surveillance).

(iv) Key management: Keys that grant access to the premises or parts thereof are only provided to trustworthy individuals, and only to the extent and as long as these persons require a separate key.

2) Detective security measures - measures to detect an attack

a) Technical Measures

(i) Scans for malware: Scans for malware (anti-virus scans) are regularly performed to identify malicious software.

(ii) Automatic checks of log files: To the extent that security log files of several systems are collected on a centralized system, log files are automatically evaluated in order to detect possible security breaches.

(iii) Security mailing lists: Any employees of the company or an external service provider are required to subscribe to relevant mailing lists for the announcement of new IT security threats (e.g., mailing lists of the manufacturers of the software used) to recognize current threat situations.

b) Organizational measures

(i) Employee security incident detection: All relevant employees are instructed on the detection and reporting of security breaches (e.g., lost computer hardware, anti-virus software alerts).

(ii) Reporting systems: There are technical procedures in place that enable employees to report anomalies and suspected security breaches of technical systems.

(iii) External persons: All employees are instructed to confront non-employees that are not accompanied by an employee should they be met on the premises in areas that are not open to visitors.

(iv) Audits: Audits and/or spot checks are performed regularly to identify potential weaknesses that could threaten the security of personal data.

(v) Checking of log files: Log files, if kept, are checked at regular intervals (e.g., with regard to unsuccessful authentication attempts).

c) Physical measures

(i) Fire alarms: To the extent appropriate with regard to the size and nature of the business facilities, fire alarms that are automatically triggered by smoke are installed.

**3)** Reactive security measures - response to an attack

a) Technical Measures

(i) Data backup: Data backups are created regularly and stored securely.

(ii) Data recovery concept: A concept for the rapid restoration of data backups has been developed in order to allow for the timely restoration of regular operation after a security breach.

(iii) Automatic removal of malware: The anti-virus software used automatically removes malware.

b) Organizational measures

(i) Reporting obligation for employees: All employees are instructed to immediately report security breaches.

(ii) Communication with external service providers: All service providers are provided with contact details to report security breaches.

(iii) Incident response process: A process has been defined to ensure adequate and timely response to security incidents. All employees have been instructed to follow that process.

c) Physical measures

(i) Fire extinguishers: There is a suitable number of fire extinguishers at the premises where personal data is processed. Employees have been made aware of the location of these fire extinguishers.

(ii) Fire alarm: In case that there is a fire detector that does not have an automatic connection to the fire department, an appropriate process ensures that the fire department can be contacted manually.

4) Deterrent security measures - measures to reduce attacker motivation

a) Technical Measures

(i) Automatic alerts: Users receive automatic alerts on risk-prone IT use (such as through the web browser if an encrypted web site does not use correct SSL / TLS certificates).

b) Organizational measures

(i) Sanctions in the case of attacks by own employees: All employees are or have been made aware that attacks on company-owned IT systems are not tolerated and that such attacks may result in serious consequences under employment law, including dismissal.

(ii) Logging of access: Any access to IT systems holding personal data is logged.

## EXHIBIT 2

## LIST OF SUB-PROCESSORS

Freshworks GmbH
Neue Grünstraße 17
10179 Berlin
Germany