DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is made effective as of Apr 24 2023 12:17 IST between the parties listed in Annex I of Schedule 1 (each a "**Party**").

(A) The Parties have entered into an agreement for the provision of services by Zoho under the online terms of service or other electronically/physically signed service agreement (the appropriate one, hereinafter "**Service Agreement**").

(B) The Parties acknowledge that, during the provision of services, personal data will be processed by Zoho. Accordingly, the Parties enter into this DPA for the purposes and scope mentioned under Clause 1 of the Schedule 1.

(C) This DPA includes the Schedule(s) and Annexures. Any reference to this DPA includes reference to the Schedule(s) and Annexures.

PARTIES HEREBY AGREE AS FOLLOWS:

1. **Instructions:** For the purposes of Clause 7.1 of the Schedule 1, Customer agrees that its instructions to Zoho for processing personal data are:

    a. to process such data strictly in accordance with the Service Agreement and this DPA;

    b. to process data where such processing is initiated by Customer via the user interface of the Zoho services;

    c. to process data for fraud prevention, spam filtering, and service improvement, including automation; and

    d. to process data to comply with other documented reasonable instructions provided by Customer (eg., via email) where such instructions are consistent with the Service Agreement and this DPA.

2. **Documentation and Compliance**

2.1 Demonstration of Compliance. Upon request by Customer, Zoho will demonstrate its compliance with GDPR and this DPA by way of reports of audits conducted in the previous 12 months by qualified and independent third party auditors, certifications approved under Article

42 of the GDPR, or approved code(s) of conduct as specified under the GDPR.

2.2 Right to Audit. Customer shall have a right to audit Zoho's data processing facilities, practices and procedures against GDPR and this DPA, provided that:
(i) Customer shall, in the first instance, always try to obtain the required information by requesting from Zoho information specified under section 2.1;
(ii) where information provided by Zoho is not sufficient to demonstrate compliance with GDPR and this DPA, Customer:

(a) shall objectively demonstrate the insufficiency by enumerating the specific obligations under GDPR and/or this DPA that are not addressed by the information provided by Zoho under section 2.1 ("Possible Compliance Gap"); and

(b) may audit Zoho's data processing facilities, practices and procedures according to the audit procedure in section 2.3; and

(iii) Customer shall reimburse Zoho for any time expended for the audit at Zoho’s then-current professional services rates, which shall be made available to Customer upon request.

2.3 Audit Procedure. The procedure for audit is agreed as follows:
(i) A reasonably specific and detailed audit plan for the Possible Compliance Gap, the proposed audit date and the duration of the audit shall be communicated to Zoho according to the notice procedure at least 30 days prior to the proposed audit date.

(ii) Zoho shall review the proposed audit plan and provide Customer with any concerns or questions along with an estimate of the charges as specified under clause (iii) of section 2.2 based on the proposed duration of audit. Zoho shall cooperate with Customer to agree on a final audit plan.

(iii) The audit shall be performed only by individuals that have an appropriate level of expertise and qualification in the subject matter to perform the audit.

(iv) The audit shall be conducted during regular business hours at the applicable data processing facility, subject to the agreed final audit plan and Zoho’s privacy, security and safety or other relevant policies and without unreasonably interfering with Zoho's business activities or compromising the security of Zoho's own data or other customers' data.

(v) Customer shall require the auditor to share the draft audit report to Zoho for review and incorporate reasonable changes suggested by Zoho.

(vi) Upon completion of the audit, Customer will promptly provide Zoho with a copy of the audit report.

2.4 Confidentiality of Information Exchanged.

(i) Customer acknowledges that all documents and information disclosed by Zoho under section 2.1, 2.2 and 2.3 and all interactions between the parties to the extent such interactions contain information about Zoho's systems and practices, including information observed or learnt by the auditor during audit and the draft and final reports ("Audit Information"), constitute Zoho's confidential information. Customer understands that unauthorized access, use or disclosure of Audit Information may cause irreparable injury to Zoho. Accordingly, Customer agrees to take, and to require the auditor engaged by Customer to take, reasonable measures to protect the confidentiality of the Audit Information from unauthorized access, use or disclosure.

(ii) Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements or confirming compliance with the requirements of this Data Processing Agreement by Zoho.

2.5 Consequences of Material Non-Compliance. In the event the audit reveals a material non-compliance by Zoho, Customer will not be required to pay the charges specified under clause (iii) of section 2.2 and Zoho shall reimburse the cost incurred by Customer for engaging the auditor for the audit.

3. Use of Sub-processors

For the purposes of Clause 7.7 of the Schedule 1:

a. The agreed list of sub-processor is published by Zoho on its websites. Customer may request Zoho for relevant information on processing by such sub-processors. Zoho shall, upon such request, make the information available to Customer.

b. Changes to the agreed sub-processor list (whether addition or replacement of a sub-processor), which apply to Customer's then current use of the service, will be communicated to Customer by email. Upon notification regarding such change by Zoho, Customer shall notify Zoho of its objection (if any) to processing by a sub-processor engaged by Zoho, in writing, within 10 business days from the date of Zoho's notice. Customer may also object in writing to processing by a sub-processor

at any time during the term of Service Agreement.

c. If Customer objects to processing by a sub-processor (as permitted by Clause 7.7 of the Schedule 1 and section 3b), Zoho will recommend to Customer commercially reasonable changes in the configuration or use of the services to avoid processing of personal data by the sub-processor. If Customer is not satisfied with the changes suggested by Zoho, Customer may, upon written notice to Zoho, terminate the Service Agreement. In the event of such termination, Zoho will refund Customer on a pro-rata basis any amounts paid by Customer for use of the service.

4. Third Parties

4.1 In addition to sub-processors, Zoho has Customer's general authorisation for the engagement of third party service providers from the agreed list published by Zoho on its websites for providing: (a) specific functionalities of Zoho services; and (b) certain essential functions such as fraud detection, spam filtering and improvement of services (**"Third Parties"**).

4.2 Customer may request Zoho for relevant information on processing by such Third Parties. Zoho shall, upon such request, make the information available to Customer.

4.3 Changes to the agreed list (whether addition or replacement of a Third Party), which apply to Customer's then current processing of personal data, will be communicated to Customer by email. Upon notification regarding such change by Zoho, Customer shall notify Zoho of its objection (if any) to processing by a Third Party, in writing, within 10 business days from the date of Zoho's notice. Customer may also object in writing to processing by a Third Party at any time during the term of Service Agreement.

4.4 If Customer objects to processing by a Third Party (as permitted by section 4.3), Zoho will recommend to Customer commercially reasonable changes in the configuration or use of the services to avoid processing of personal data by the Third Party. If Customer is not satisfied with the changes suggested by Zoho, Customer may, upon written notice to Zoho, terminate the Service Agreement. In the event of such termination, Zoho will refund Customer on a pro-rata basis any amounts paid by Customer for use of the service.

5. International Transfers

5.1 For the purposes of Clause 7.8, Customer understands that personal data; (i) will be stored in

Zoho's data centers in the European Economic Area (EEA); (ii) may be accessed on a need basis by applicable Zoho group entities as described in Schedule 2; and (iii) will be transferred outside EEA to the sub-processors and Third Parties depending on the Zoho services used by Customer. Customer agrees that such transfers of personal data are necessary for providing the services and will be deemed as instructions by Customer.

5.2 Where Zoho transfers personal data to Zoho group entities, sub-processors, or Third Parties located outside EEA, Zoho shall ensure that a valid basis of transfer as required by GDPR is in place.

6. Data Subject Requests

6.1 For the purposes of Clause 8 (a), Customer authorizes Zoho to respond to the requests from data subjects before notifying Customer, to determine if the request is with respect to the personal data processed by Zoho on behalf of the Customer.

6.2 For the purposes of Clause 8(b), Zoho shall implement technical and organizational measures to enable Customer to comply with requests from data subjects who wish to exercise their rights such as right to restrict Processing, right to erasure, right to rectification, right to access, right not to be subject to an automated individual decision making or data portability. Where Customer requests Zoho's assistance (under this section and Clause 8) and Zoho has already enabled Customer to comply with such requests by implementing appropriate technical and organizational measures, Zoho shall have the right to charge the Customer for any reasonable costs or expenses incurred by Zoho in order to assist Customer with request(s) from data subjects.

7. Other Assistance to the Controller

7.1 For the purposes of Clause 8(c), Parties agree that Zoho's obligation to assist Customer in its obligation to (i) conduct a data protection impact assessment; and (ii) consult the competent supervisory authority/ies, is limited to providing the relevant information to Customer.

7.2 For the purposes of Clause 9.1, Parties agree that Zoho's obligation to assist the Customer in notifying the supervisory authority and in notifying the data subjects is limited to, (i) the extent such breach involves personal data processed by Zoho on behalf of the Customer; and (ii) providing relevant information about the breach to Customer, if such information is available to Zoho and otherwise not available to Customer.

8. Return and Deletion of Data

For the Purposes of Clause 10(d), Customer acknowledges and agrees that:

a. Return of personal data processed by Zoho should be achieved via Customer initiating the export of such personal data via the user interface made available by Zoho;

b. Zoho will automatically delete personal data processed by Zoho at the next routine clean-up cycle from the primary servers (that occurs once in 6 months). The data deleted from primary servers will be deleted from backups 3 months thereafter; and

c. Zoho will provide confirmation of the completion of the relevant clean-up cycle as certification of deletion of the personal data. Such certificate will be provided only upon request from Customer.

9. Governing Law and Jurisdiction

9.1 This DPA shall be governed by and construed strictly in accordance with the laws of the Federal Republic of Germany, excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG) of 11 April 1980 and excluding the conflict of law provisions of German private international law as amended from time to time.

9.2 Any dispute arising out of or resulting from this Agreement shall be subject to the exclusive jurisdiction of courts in Düsseldorf to the exclusion of all other courts.

10. DPA to Supersede Prior Agreements

Parties agree that this DPA will supersede and prevail over all the previous data protection and privacy agreement(s) between Customer and Zoho.

SCHEDULE 1
STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1 (Purpose and scope)

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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, and repealing Directive 95/46/EC (General Data Protection Regulation/"GDPR").

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of GDPR.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of GDPR.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of GDPR.

Clause 2 (Invariability of the Clauses)

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(**b)** This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 (Interpretation)

(a) Where these Clauses use the terms defined in GDPR, those terms shall have the same

meaning as in GDPR.

(b) These Clauses shall be read and interpreted in the light of the provisions of GDPR.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in GDPR or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 (Hierarchy)

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

Clause 5 (Docking clause)

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6 (Description of processing(s))

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 (Obligations of the Parties)

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe the GDPR or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the 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 and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from GDPR. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor

complies with the obligations to which the processor is subject pursuant to these Clauses and to GDPR.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of GDPR.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of GDPR, the processor and the sub-processor can ensure compliance with Chapter V of GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of GDPR, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 (Assistance to the controller)

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the

controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) The obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) The obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) The obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) The obligation in Article 32 of GDPR.

(5) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 (Notification of personal data breach)

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of GDPR, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) In notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) In obtaining the following information which, pursuant to Article 33(3) of GDPR, shall be stated in the controller's notification, and must at least include:

(1) The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) The likely consequences of the personal data breach;

(3) The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) In complying, pursuant to Article 34 of GDPR, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller’s obligations under Articles 33 and

34 of GDPR.

SECTION III

FINAL PROVISIONS

Clause 10 (Non-compliance with the Clauses and termination)

(a) Without prejudice to any provisions of GDPR, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) The processor is in substantial or persistent breach of these Clauses or its obligations under GDPR.

(3) The processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to GDPR.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Controller(s): [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]*

Name: aiio GmbH

Address: Klausenerstraße 10a, 39112 Magdeburg, Germany

Signature Jobst von Heintze

Name Jobst von Heintze

Title CMO

Date Apr 24 2023 12:17 IST

Contact jobst.von.heintze@aiio.de

Processor(s):

Name: Zoho Corporation GMBH**("Zoho")**

Address: Trinkausstr. 7, 40213 Dusseldorf, Germany

Signature S. Iyengar

Name Sridhar Iyengar

Title Director

Date Jan 13 2022 13:26 IST

Contact privacy@eu.zohocorp.com

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed:

The personal data processed concern the following categories of data subjects:

Zoho may process any data inputted by authorised users of Zoho's online collaboration and management tools. Primarily, this will relate to living individuals who are:

- users who are authorised by Customer to use the services
- employees, agents, contractors, and contacts of the Customer
- prospects, customers and clients, business partners and vendors of the Customer
- advisers and professional experts of the Customer
- employees, agents, contractors, and contacts of the Customer's prospects, customers and clients, business partners, vendor, advisers and professional experts.

Categories of personal data processed:

Categories of personal data processed may include, but are not limited to:

- Name, contact details, address
- Employment related data
- Financial information

Sensitive data processed (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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

Zoho provides options to encrypt sensitive data at rest. The ability to encrypt data at rest is different in each Zoho service and it may not be enabled by default. The details of encryption capabilities in Zoho services are either published by Zoho on its websites or available to

Customer upon request. Based on the nature of the sensitive personal data processed, Customer shall determine the suitability or adequacy of encryption capabilities provided by Zoho service(s) and enable encryption.

Nature of the processing: The nature of processing by Zoho will include the provision of Zoho services pursuant to the terms of Service Agreement, this DPA or any other agreement between Customer and Zoho.

Purpose(s) for which the personal data is processed on behalf of the controller: To provide Zoho services in accordance with instructions provided by Customer as described under section 1 of this DPA.

Duration of the processing: Duration of the Service Agreement

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing:
As specified under section 3, Sub-processor(s) will process personal data for the duration of the Service Agreement.

ANNEX III

Technical and organisational measures including technical and organisational measures to ensure the security of the data

Technical and Organizational Security Measures Implemented by Zoho

Zoho has established, and will maintain at a minimum, an information security management system that includes the following:

Security Governance

1. A governance framework that supports relevant aspects of information security through appropriate policies and standards.
2. Formal documentation of the roles and responsibilities of employees with respect to governance of Information Security within Zoho that are communicated by the management to employees.
3. An information security program in accordance with the international standard ISO 27001 that includes technical, organizational and physical security measures in order to protect personal data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction.
4. Formally documented information security policy, data privacy policy and other policies that are communicated periodically to employees responsible for the design, implementation and maintenance of security and privacy controls. The policies will be reviewed annually to keep them up-to-date.
5. Compliance with industry standard security measures as described at https://www.zoho.com/compliance.html.

Risk Management

1. Annual risk assessment, to prioritize mitigation of identified risks.
2. Established internal audit requirements and periodical audits on information systems and processes at planned intervals.
3. Assessment of the design and operating effectiveness of controls against the established control framework through which corrective actions related to identified deficiencies will be tracked to resolution.

Human Resources Security

1. Background verification of all employees having access to confidential data that includes verification of criminal records, previous employment records if any, and educational background.
2. Signing of confidentiality agreement and acceptable use policy by employees upon their employment with clauses on protection of confidential information.
3. Training on security and privacy awareness including training on Zoho's policies, standards and relevant technologies along with maintenance and retention of training completion records.
4. Employees will be required to adhere to the information security policies and procedures. Disciplinary process for non adherence will be defined and communicated.

Identity and Access management of Zoho Personnel

1. Creation of unique identifiers for employees to access information systems and prohibition of sharing user accounts among employees.
2. User authentication to information systems protected by passwords that meet Zoho's password policy requirements derived based on NIST SP 800-63B standards.
3. Strong password configurations that include i) 8 character minimum length; ii) non dictionary words and iii) screening of passwords against list of known compromised passwords.
4. Mandatory Two factor authentication for access to information systems involving confidential data.
5. Secure remote access to the corporate network provisioned via SSL VPN with strong encryption and two factor authentication.
6. Adherence to the principles of least privilege and need-to-know and need-to-use basis for access control.
7. Approval mechanism from appropriate personnel to provide access to information systems.
8. Revocation of access that is no longer required in the event of termination or role change.
9. Recording of approval, assignment, alteration and withdrawal of access rights.
10. User access reviews on a half yearly basis and corrective actions whenever necessary.
11. Restrictions on administrative access to personal data and provision of access on a strictly need-to-know basis along with implementation of access-control measures such as mandatory two factor authentication.

Asset Management

1. Inventory maintenance of assets associated with information processing. Owners are

assigned for each asset and rules for acceptable use of assets are defined. Assets assigned to employees are returned in the event of termination or role change.

2. Capacity management policies through which resources are continuously monitored and projections are made for future requirements.
3. Determined procedures in accordance with industry best practices for the reuse, secure disposal and destruction of electronic media to ensure that the data is rendered unreadable and unrecoverable.
4. Disposal of unusable devices by verified and authorized vendors which includes storing of such devices in a secure location until disposal, formatting any information contained in the devices before disposal, degaussing and physical destruction of failed hard drives using shredder and crypto-erasing and shredding of failed SSDs.

Physical Security

1. Physical access to Zoho's data center is highly restricted and requires prior management approval. The data centers are housed in facilities that require electronic card key access. Additional two-factor authentication and biometric authentication are required to enter the data center premises and there is continuous monitoring of CCTV cameras and alarm systems.
2. Control of physical access to Zoho's development facilities using access cards and monitoring by security personnel.
3. Installation of CCTV cameras and review of access logs and CCTV footage in case of any incidents.
4. Defined visitor management process to authorize visitor entries and maintenance of access records of visitors.
5. Revocation of physical access to employees in the event of termination of employment or role change.

Network Security and Operations

1. A dedicated Network Operations Center (NOC), which operates 24x7 monitoring the infrastructure health.
2. Establishment and implementation of firewall rules in accordance to identified security requirements and business justifications.
3. Review of firewall rules on a quarterly basis to ensure that legacy rules are removed and active rules are configured correctly.
4. Establishment and maintenance of appropriate network segmentation, that includes use of virtual local area networks (VLANS) where appropriate, to restrict access to systems

storing confidential data with a data storage layer that is designed to be not directly accessible from the Internet.

5. Clear separation of production, development and integration environments to ensure that production data is not replicated or used in non-production environments for testing purposes.
6. Management of access to production environments by a central directory and authentication for such access using a combination of strong passwords, two-factor authentication, and passphrase-protected SSH keys. Access to the production environment is facilitated through a separate network with strict rules.
7. Deployment of DDOS mitigation capabilities from well established service providers to prevent volumetric attacks and to keep the applications available and performing.

Secure Software Development

1. Well defined security process that is implemented and monitored throughout the SDLC taking into consideration confidentiality, availability and integrity requirements.
2. Implementation of secure software development policies, procedures, and standards that are aligned to industry standard practices such as OWASP, CSA, CWE/SANS including secure design review, secure coding practices, risk based testing and remediation requirements.
3. Training on secure coding principles and industry standards to personnel involved in the development and coding of products.
4. "Secure by design" approach by incorporating security risk assessments and Threat modeling in the planning and analysis phase of SDLC and review of the design to prevent new threats.
5. Examination of Source code changes for potential security issues using Zoho's proprietary SAST (static code analysis) tools and manual review process before deployment.
6. Web Application Firewall (WAF) layer that is embedded in all web applications for protection against Open Web Application Security Project (OWASP) threats, including SQL injections, Cross-site scripting (XSS) and remote file inclusions.
7. Maintenance of inventory of third party software that gets bundled in the products/services.
8. Alerts on potential security vulnerabilities in the third party software by Zoho's proprietory SCA (Software Composition Analysis) that is reviewed periodically to check its applicability and impact and to take steps to upgrade third party software to the latest version.
9. Appropriate checking and elimination procedures to ensure that the service is not affected

by malware/viruses during development, maintenance and operation.

10. Appropriate security controls to ensure the confidentiality, integrity and availability of the CI/CD pipeline in the software development environment used to develop, deploy, and support the products.
11. Maintenance of clear distinction between the development, QA and production environments.

Data Security and Management

1. Information classification scheme with data handling guidelines related to access control, physical and electronic storage, and electronic transfer.
2. Logical separation of each customer's service data from other customers' data by distributing and maintaining separate logical cloud space for each customer.
3. Deletion of data from active database upon termination of Zoho services by the customers (clean-up occurs once in every 6 months), deletion of backup data within 3 months of deletion from active database and termination of accounts that remain unpaid and inactive for a continuous period of 120 days by giving prior notice to the customer.

Cryptography

1. Use of transport encryption for information that traverses across networks outside of the direct control of Zoho including, but not limited to the Internet, Wi-Fi and mobile phone networks.
2. Encryption of data transmission to Zoho services are made using TLS 1.2/TLS1.3 protocols, with latest and strong ciphers like AES_CBC/AES_GCM 256 bit/128 bit keys, authentication of message using SHA2 and use of ECDHE_RSA as the key exchange mechanism.
3. Encryption of sensitive data at rest using 256-bit Advanced Encryption Standard (AES). (The data that is encrypted at rest varies specific to Zoho services and also options are provided where the customer defines the fields to encrypt depending on their business need and data sensitivity).
4. Irreversible industry standard algorithm (bcrypt) will be used to hash and store the passwords of Zoho services with randomly generated per user salt added to the input.
5. Zoho's in-house Key Management Service (KMS) to own and maintain encryption keys that includes additional layer of security by encrypting the data encryption keys using master keys.
6. Separation of master keys and data encryption keys by physically storing them in different servers with limited access.

Change Management

1. A change management policy that governs changes in all components of the service environment whereby all changes are planned, tested, reviewed and authorized before implementation into production.
2. Assessment of the potential impacts, including information security and privacy impacts of the changes.
3. Documented fall-back mechanisms including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
4. Notification to customers of any changes that may affect customers in an adverse manner.

Configuration Management

1. Implementation of security hardening and baseline configuration standards in accordance with industry standards that are reviewed and updated periodically.
2. Predefined OS images with security baselines are used to build systems in development and production.
3. Hardening standards including (i) ensuring that unnecessary features, services, components, files, protocols and ports are removed from the production environment; and (ii) removing unnecessary user logins and disabling or changing default passwords.
4. Approval from the appropriate personnel to install any software package in the production environment.

Vulnerability Management

1. Vulnerability management plan designed to (i) identify promptly, prevent, investigate, and mitigate any cyber security vulnerabilities; (ii) analyze the vulnerability; (iii) perform recovery actions to remedy the impact.
2. Vulnerability assessments using automated scanners performed periodically on Zoho's internet facing systems.
3. Application penetration testing by Zoho's in house security personnel performed annually in accordance to defined test methodologies.
4. Review of identified issues from vulnerability assessments and penetration testing, determination of its applicability, impact and priority and rectification in accordance with the SLA definition:High level vulnerabilities within 7 calendar days of discovery, Medium level vulnerabilities within 30 calendar days of discovery and Low level vulnerabilities within 60 calendar days of discovery.

5. Monitoring known vulnerabilities from common sources such as OWASP, CVE, NVD and other vendor security lists and installation of security relevant patches to product and/or supporting systems in accordance with Zoho's patch management policy.
6. Antivirus deployment by running the current version of industry standard anti-virus software as a part of which signature definitions are updated periodically within 24 hours of release, real time scans are enabled and alerts are reviewed and resolved by appropriate personnel.

Security Logging and Monitoring

1. Use of centralized logging solution to aggregate and correlate events from various components including network devices, servers and applications.
2. Maintenance of audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events and retention of logs in accordance with applicable policies and regulations.
3. Host and application intrusion detection (IDS) technology to facilitate timely detection, investigation and response to incidents.
4. Restrictions on physical and logical access of logs by authorized personnel.

Business continuity and Disaster recovery

1. Disaster recovery and business continuity plans and processes (i) to ensure continuous availability of the services in case of any disaster; (ii) to provide an effective and accurate recovery.
2. Annual review of business continuity plan to evaluate its adequacy & effectiveness.
3. Redundancy mechanisms to eliminate single point of failure consisting of (i) dual or multiple circuits, switches, networks or other necessary devices; and (ii) storing of application data in a resilient storage that is replicated in near real time across data centers.
4. Taking periodic backups (incremental backups every day and weekly full backups) and storing them in an encrypted format in the same datacenter.
5. Retention of backups for a period of three months and testing recovery of backups at planned intervals.
6. SLA for service availability with 99.9% monthly uptime as a part of which real time availability can be viewed in https://status.zoho.com.

Incident Management

1. An incident response plan and program containing procedures that are to be followed in

the event of an information security incident.

2. Dedicated email (incidents@zohcorp.com) to which external parties can report security incidents and creating awareness among employees to report any potential security incident or weakness on time without any delay.
3. Tracking of security incidents, fixing of such incidents through appropriate actions, maintenance of such records in the incident registry and implementation of controls to prevent recurrence of similar incidents.
4. Incident management procedures that lays down the steps for notifying the client, and other stakeholders in a timely manner in accordance with breach notification obligations.
5. Implementation of appropriate forensic procedures including chain of custody for collection, retention, and presentation of evidence in the event of an information security incident likely to result in a legal action.

Third-Party Vendor Management

1. Vendor management policy through which Zoho evaluates and qualifies third party vendors as a part of which new vendors are onboarded only after understanding their processes and performing risk assessments.
2. Execution of agreements with vendors that require vendors to adhere to confidentiality, availability, and integrity commitments in order to maintain Zoho's security stance.
3. Annual reviews to monitor the operation of vendor's processes and security measures.

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller: As specified under section 7 of the DPA

ANNEX IV
List of sub-processors
(NOT APPLICABLE)

EXPLANATORY NOTE:

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).

The controller has authorised the use of the following sub-processors: **NOT APPLICABLE**

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

SCHEDULE 2
APPLICABLE GROUP ENTITIES

Applicable to	**Access by**	**Purpose**
Customers from the EEA	Zoho group entities in India	For support and debugging
Customers from Spain	Zoho group entities in Mexico and Columbia	For providing support in regional language
Customers from Portugal	Zoho group entities in Brazil	For providing support in regional language
Customers from France	Zoho group entities in Dubai	For providing support in regional language