DATA PROCESSING ADDENDUM

14 May 2025

This Data Processing Addendum ("**Addendum**" or the "**DPA**") is incorporated into and forms part of the Zensai Software-as-a-Service Agreement, meaning the Standard Terms and Conditions, together with the Quote and any incorporated documents (the "**Agreement**") and is entered into between the Data Controller ("**Customer**" or the "**Controller**"), meaning the customer as set out in the Agreement, and the Data Processor ("**Zensai**" or the "**Processor**"), meaning the Zensai legal entity as set out in the Agreement (also individually named a "**Party**" and collectively the "**Parties**").

The DPA consists of this main Addendum and the following Annexes and Appendices:

Annexes:

Annex I	Description of the Processing
Annex II	List of Sub-processors
Annex III	Technical and Organizational Measures including Measures to ensure the Security of the Data
Annex IV	Additional terms

Appendices – for transfers to third countries:

Appendix 1	EU Commission SCC Module 4: Processor to Controller
Appendix 2	UK Transfer Addendum to the EU SCC
Appendix 3	Swiss Adaption to the EU SCC

1. PURPOSE AND SCOPE

1.1 The DPA governs the processing of personal data in connection with the Services provided under the Agreement. The DPA is applicable when the Controller or Processor is subject to 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 or the "GDPR"). In the event that neither party is subject to the GDPR, but other Data Protection Legislation is applicable to the Services, the terms of the DPA shall be construed and applied to ensure compliance with those laws. Capitalised terms not defined in the DPA have the meaning as set out in the Agreement.

1.2 The purpose of the DPA is to ensure compliance with applicable Data Protection Legislation for performance of the Services. "Data Protection Legislation" means the applicable local, state, federal, or international laws and regulation, or treaties relating to the privacy, security or protection of personal data, as may be defined in such laws.

1.3 The DPA is drafted to comply with Article 28(3) and (4) of the GDPR. For compliance with other Data Protection Legislation when applicable to the Services, the relevant national legislation adopted with the DPA by reference in appendices shall apply in addition to the main part of this DPA.

1.4 For all personal data processed by Zensai in connection with the Services, the Parties intent that the Customer is the Controller and Zensai is the Processor as the provider of the Services. An affiliate of the Processor may, with the agreement of the Controller, accede as a party to the DPA under the terms and procedure stated in Section 1, Clause 5, (*the Docking Clause*).

1.5 The DPA are without prejudice to obligations to which the Controller is subject to under Data Protection Legislation. In connection with its access to and use of the Services, the Controller shall process personal data within such Services and provide Zensai with appropriate instructions in accordance with such Data Protection Legislation applicable to the Controller.

1.6 Where Zensai is processing personal data as a Controller, the Zensai Privacy Policy shall apply to such processing and not this DPA.

1.7 Transfers of personal data out of the EU/EEA, the UK or Switzerland (the "European Area") and into third countries are subject to the EU Commission adopted Standard Contractual Clauses (the "EU SCC") for transfers of personal data to third countries pursuant to Article 46(2)(c) of the GDPR, with the addition of

and subject to the UK Transfer Addendum to the EU SCC (Appendix 2) as applicable for transfers out of the UK, and the Swiss amendments as stated in the Swiss Adaption to the EU SCC (Appendix 3) as applicable for transfers out of Switzerland.

1.8 In the event that Zensai transfers personal data out of the European Area to customers placed in third countries, the EU SCC Module 4 ("Processor to Controller") (Appendix 1) shall apply to the transfer and is incorporated by reference and the EU SCC with appendices can be downloaded – see reference via Appendices. For transfers to the US to customers who have self-certified under the EU-US Privacy Framework, this framework shall apply.

2. INVARIABILITY OF THE DPA

2.1 The Parties undertake not to modify the DPA, except for adding information to the Appendices and Annexes or updating information in them.

2.2 The Appendices and Annexes form an integral part of the DPA. The Parties may in the Appendices and Annexes add clauses or additional safeguards provided that they do not directly or indirectly contradict the main terms of the DPA or detract from the fundamental rights or freedoms of data subjects.

3. INTERPRETATION

3.1 Where the DPA uses the terms defined in the GDPR, those terms shall have the same meaning as in the GDPR.

3.2 The terms of the DPA shall be read and interpreted in the light of the provisions of the GDPR. References to "Member States" shall include all EEA Member States.

3.3 The terms of the DPA shall not be interpreted in a way that runs counter to the rights and obligations provided for in the GDPR or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4. HIERARCHY

4.1 The DPA supplements and amends and forms part of the Agreement.

4.2 If the DPA or any of its terms is inconsistent or in contradiction with any other provisions of the Agreement, the terms of the DPA shall prevail.

4.3 In the event of a conflict between the DPA or any other provision of the Agreement and the EU SCC, the EU SCC shall control.

5. DOCKING CLAUSE

5.1 Any entity that is not a Party to the DPA may, with the agreement of all the Parties, accede to the DPA at any time as a Controller or a Processor by completing and signing the Annexes.

5.2 Once the Annexes in 5.1 are completed and signed, the acceding entity shall be treated as a Party to the DPA and have the rights and obligations of a controller or a Processor.

5.3 The acceding entity shall have no rights or obligations resulting from the DPA from the period prior to becoming a Party.

6. DESCRIPTION OF PROCESSING(S)

6.1 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 I.

7. OBLIGATIONS OF THE PARTIES

7.1 Instructions

(i) The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by the EU 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.

(ii) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe the GDPR or the applicable EU or Member State data protection provisions.

7.2 Purpose limitation

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

7.3 Duration of the processing of personal data

(i) Processing by the Processor shall only take place for the duration specified in Annex I and Annex III.

7.4 Security of processing

(i) 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.

(ii) 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 DPA. 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

(i) 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

(i) The Parties shall be able to demonstrate compliance with the DPA.

(ii) The Processor shall deal promptly and adequately with inquiries from the Controller about the processing of data in accordance with the DPA.

(iii) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in the DPA and stem directly from the GDPR. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by the DPA, 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.

(iv) 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.

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

7.7 Use of sub-processors

(i) General written authorisation: 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.

(ii) 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 Processor in accordance with the DPA. The Processor shall ensure that the sub-processor complies with the obligations to which the Processor is subject pursuant to the DPA and to the GDPR.

(iii) 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.

(iv) 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.

7.8 International transfers

(i) 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 EU or Member State law to which the Processor is subject and shall take place in compliance with Chapter V of the GDPR.

(ii) 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 the GDPR, the Processor and the sub-processor can ensure compliance with Chapter V of the GDPR by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of the GDPR, provided the conditions for the use of those standard contractual clauses are met.

8. ASSISTANCE TO THE CONTROLLER

8.1 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 the Controller.

8.2 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 8.1 and 8.2, the Processor shall comply with the Controller's instructions.

8.3 In addition to the Processor's obligation to assist the Controller pursuant to Clause 8.2, 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:

(iii) 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;

(iv) 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;

(v) 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;

(vi) the obligations in Article 32 of the GDPR.

8.4 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.

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 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, 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 a personal data breach concerning data processed by the Controller, the Processer shall assist the Controller:

(i) 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);

(ii) in obtaining the following information which, pursuant to Article 33(3) of the 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.

(iii) 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.

(iv) in complying, pursuant to Article 34 of the 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 Processer shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

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

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

(iii) 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 the GDPR.

10. NON-COMPLIANCE WITH THE DPA AND TERMINATION

10.1 Without prejudice to any provisions of the GDPR, in the event that the Processor is in breach of its obligations under the DPA, the Controller may instruct the Processor to suspend the processing of personal data until the latter complies with the DPA or the Agreement is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with the DPA, for whatever reason.

10.2 The Controller shall be entitled to terminate the affected Services in accordance with the termination provisions in the Standard Terms and Conditions, Section 17 insofar as it concerns processing of personal data in accordance with the DPA if:

(i) the processing of personal data by the Processor has been suspended by the Controller pursuant to point 10.1 and if compliance with the DPA is not restored within a reasonable time and in any event within one month following suspension;

(ii) the Processor is in substantial or persistent breach of the DPA or its obligations under the GDPR;

(iii) the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to the DPA or to the GDPR.

10.3 The Processor shall be entitled to terminate the Agreement insofar as it concerns processing of personal data under the DPA where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (ii), the Controller insists on compliance with the instructions.

10.4 Following termination of the DPA, 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 the EU 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 the DPA.

11. GOVERNING LAW AND VENUE

11.1 The DPA with its Annexes and Appendices is governed by and shall be construed and enforced in accordance with the laws as set out in the Standard Terms and Conditions, Section 18.1.

11.2 The venue shall be the courts as set out in the Standard Terms and Conditions, Section 18.2.

12. COMMENCEMENT AND TERMINATION

12.1 The DPA shall come into effect on the date of concluding the Agreement.

12.2 Each Party shall be entitled to require the DPA renegotiated if changes to the EU or Member State law, or inexpediency of the DPA should give rise to such renegotiation.

12.3 The DPA shall apply for the duration of the Services, and the DPA cannot be terminated unless another data processing agreement governing the personal data processing with the Services have been agreed by the Parties.

12.4 If the Services under the Agreement is terminated, and the personal data is deleted or returned to the Controller pursuant to Clause 10.4 and Annex III.4., the DPA may be terminated by written notice by either Party.

ANNEX I: DESCRIPTION OF THE PROCESSING

I.1 The purpose for which the personal data is processed on behalf of the Controller is:

The Customer, as the Controller and Zensai, as the Processor have entered into the Agreement pursuant to which the Controller is granted a license to access and use the Service for the duration of the subscription term. In providing the Service, the Processor will, on behalf of the Controller, process personal data submitted to and stored within the Service by the Controller or third parties being users with whom the Controller provides access to apply the Service under its license.

I.2 The nature of the processing:

Zensai will as the Processor host and process personal data in the course of providing its cloud-based services to the Controller as Learn365, Engage365, Perform365, Integrate365 & Flow365. Additional services offered as Services of the Processor and subscribed to by the Controller, could include applications to Learn365, Engage365, Perform365, Integrate365 & Flow365 and other additional applications & services. Included in Learn365, Perform365, Engage365, Integrate365 & Flow365 are optional generative AI features based on the principles stated in Annex III.2.

I.3 Categories of data subjects whose personal data is processed:

The processing on behalf of the Controller involves personal data about the following categories of data subjects:

- Employees of the data Controller, to also include agents, consultants, freelancers;
- Other users of the Services when authorised by the Controller under the terms of the Agreement;
- Individuals to the extent identifiable in the context of emails or messaging content when using the Services or in archiving content; and
- Recipients of communication who are natural persons, when the Services is applied for communication.

I.4 Categories of personal data processed

I.4.1 General personal data

Learn365 processes the following data submitted by or under the authorisation of the Controller of relevance to the Services:

- Account name
- User display name
- Email address
- Department
- Job title
- Office
- Country
- City
- Manager ID/email
- Training records *
- Competencies

* Training records consist of information about which training a learner has historically enrolled into, started and/or completed. This includes data on pass/fail information of assessments as well as assessment scores, if used.

Specifically, for the Perform365 & Engage365-Services, the following personal data may also be processed:

- Full name
- Unique identifiers (username, account number, password)
- Manager ID
- Office and geolocation based upon IP address
- Profile photo
- Education and profession

- Survey, feedback and assessment messages
- Performance data and assessments
- Task and objective data used in assessing performance
- Personal data added or derived from use of the service such as records and business intelligence information
- Personal data within emails or messaging content or file attachments or support enquiries which identifies or may reasonably be used to identify data subjects

I.4.2 Special categories of personal data

Learn365, Perform365, Engage 365, Integrate365 and Flow365 does not collect sensitive personal data as defined in Article 9 of the GDPR as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade or union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Neither does Learn365, Perform365, Engage 365, Integrate365 or Flow365 collect special categories of personal data such as records of criminal offenses and convictions nor personal social security numbers or other government issued personal identification numbers.

The Services are not aimed at nor designed for processing special categories of personal data, and sensitive personal data are not naturally occurring types of information for purpose of the Services. The Controller will determine the content when using the Services and shall advise its user on the categories of personal data to submit to the content and securities measures to apply. Should the Controller, at its sole discretion, choose to submit personal data to the content that constitutes special categories of personal data or sensitive personal data, the Controller shall remain solely responsible for ensuring that any such personal data is lawfully obtained and that its submission and processing comply with applicable laws and regulations.

I.5 Duration of the processing

The processing of personal data on behalf of the Controller commences upon the initiation of the Services and will continue for the duration of the Agreement with delivery of Services.

Following termination of the Services, the personal data will be processed according to the procedures for storage, retention, and deletion as stated in Annex III.4.

ANNEX II: LIST OF SUB-PROCESSORS

II.1 Approved sub-processors

The Processor has the Controller's general authorisation for the engagement of sub-processors following the processing stated in the DPA, Clause 7.7(i).

On commencement of the Services, the Controller authorises the engagement of the sub-processors which the Processor may apply for processing the Services ordered.

The list of approved sub-processors is available on the Processor's website here.

If the Controller has reasonable grounds to object to the Processor's use of a new sub-processor, the Controller shall notify the Processor in writing within fourteen (14) days after the Processor has informed the Controller of its plans to engage the sub-processor. The parties shall then discuss the Controller's concerns in good faith with the aim of reaching a commercially reasonable resolution. If no such resolution can be achieved, the Controller shall be entitled to terminate the affected Services in accordance with the termination provisions in the Standard Terms and Conditions, Section 17.

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING MEASURES TO ENSURE THE SECURITY OF THE DATA

III.1 The subject of/instruction for the processing

The processing of personal data on behalf of the Controller shall be carried out by the Processor under the instructions stated in this Annex III.

The instructions cover the processing of the categories of data for performance of the Services ordered by the Controller, and as listed in Annex I.

The Services including its components, features and other applications shall serve the purpose to deliver and manage services (add, use, record, store, edit, structure, organise, analyse, export and delete personal data) on behalf of the Controller and its authorised users.

III.2 Security of processing

The level of security shall take into account the nature, scope, context and purposes of the processing activity, as well as the risk for the rights and freedoms of natural persons.

Since processing activities involve processing of personal data a high level of security has been established. The data Processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The Processor shall implement and maintain the technical and organizational measures set out in this Annex III and described on the Processor's website here. The Processor shall ensure that sub-processors apply security measures that provide at least an equivalent level of protection. These measures are hereby incorporated into this DPA by reference. The Processor shall maintain and update these technical and organizational measures as necessary.

The Processor's approach to AI and data privacy is described here, and forms part of its overall security framework.

III.3. Assistance to the Controller

The Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Controller in accordance with the DPA, Clause 8 by implementing the following:

Appointed responsible for assistance to the Controller
The Processor has established an internal organisation dedicated to ensuring compliance with its obligations to the Controller.

Data subject request
The Processor shall inform the Controller in writing (email is acceptable) of any requests received from a data subject concerning their rights under the GDPR, as they pertain to the data processor's processing activities on behalf of the Controller. Read more about our data subject request here.

Data breach detection and notification
In the event of a breach, i.e. a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, the Processor will, without undue delay, but no later than in 48 hours after becoming aware of the breach, notify the Controller in writing (email is acceptable).

The breach notification will contain at least the information set out in Clause 9.2. Where, and as far as, it is not possible to provide the information listed at the same time, the information may be provided in phases without undue further delay.

The Processor takes all the necessary steps to protect the data after having become aware of the breach. The Processor will cooperate with the Controller, and with any third parties designated by the Controller, to respond to the breach. The objective of the breach response will be to restore the confidentiality, integrity, and availability of all Zensai Services, to establish root causes and remediation steps, to preserve evidence and to mitigate any damage caused to data subjects or the Controller. Read more here.

III.4 Storage period / erasure procedures

Personal data shall be retained only for the duration necessary to fulfil the purposes for which it was originally collected, and thereafter solely as required for legal and regulatory compliance, or as mandated by applicable law. Following the termination of the Services, the provisions of this DPA shall continue to apply until the personal data is fully deleted. Detailed information regarding erasure procedures and specific timelines for erasure is available on the Processor's website here.

III.5 Processing location

Processing of the personal data under the DPA cannot be performed at other locations than (i) the Processor's own locations, (ii) the Microsoft Azure Data Centers selected by the Controller at installation, as described in the Processor's Trust Center here, and (iii) the locations of authorised sub-processors as referred to in Annex II, without the Controller's prior written authorisation.

III.6 Instruction on the transfer of personal data to third countries

By entering into this DPA, the Controller agrees that the Processor transfers personal data to and stores personal data in third countries to the extent necessary using the sub-processors listed in Annex II.

If the Controller does not in the DPA or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the Processor shall not be entitled within the framework of the DPA to perform such transfer.

III.7 Procedures for the Controller's audits, including inspections, of the processing of personal data being performed by the Processor

The Controller is entitled to verify Zensai's compliance with the GDPR and the DPA by requesting a certificate, such as ISO27001/ISO27701 or SOC2 certification, reflecting the results of an audit conducted by an independent third-party auditor. This certificate, or a comparable certification, must be issued within twelve (12) months from the date of the Customer's request.

In cases where the documentation provided are insufficient to demonstrate compliance, the Processor shall, upon prior reasonable written notice and no more than once per calendar year, provide access to a reputable auditor nominated by the Controller. This auditor will be granted access to the necessary information to reasonably demonstrate compliance with the DPA and may conduct audits, including inspections, related to the processing of personal data for performance of the Services. The auditor must adhere to standard confidentiality obligations, including those towards third parties. The Processor reserves the right to object to an auditor nominated by the Controller if the Processor reasonably believes the auditor lacks suitable qualifications or is a competitor of the Processor.

The Controller shall bear all costs associated with the Audit and ensure that the auditor avoids causing any damage, injury, or disruption to the Processor's premises, equipment, personnel, and business during the audit process.

The DPA does not require the Processor to disclose or grant access to the Controller or its third-party auditor to: (i) any data belonging to other Zensai customers; (ii) Zensai's internal accounting or financial information; (iii) any trade secrets of Zensai or its affiliates; (iv) any information that, in Zensai's reasonable opinion, could compromise the security of Zensai's systems or breach its obligations under applicable law or its security or privacy obligations to third parties; or (v) any information that the Controller or its third-party auditor seeks to access for reasons other than fulfilling the Controller's obligations under the GDPR and the DPA in good faith.

III.8 Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The Processor is responsible for determining how to monitor the sub-processors compliance with the GDPR and the DPA. This includes deciding on the type of auditor's reports or certificates to be obtained and whether physical inspections shall be conducted.

The monitoring approach and its extent should be tailored to reflect the nature, scope, context, and purposes of the processing activities undertaken by the sub-processors, as well as the risks they pose to the rights and freedoms of individuals, considering their likelihood and severity.

The Processor will perform an audit or inspect the sub-processors at least annually.

At the Controller’s written request, the Processor will provide the Controller with a confidential summary of the documentation of these audits or inspections (“Summary Report”).

ANNEX IV ADDITIONAL TERMS OF AGREEMENT

IV.1. Documentation

The DPA along with Annexes and Appendices shall be retained in writing, including electronically, by both Parties.

IV.2 Assistance to the Controller and extra documentation

The Processor's assistance to the Controller in accordance with Clause 8 and regarding "extra documentation" in Annex III, Clauses IV.7 and IV.8 is remunerated. The remuneration is calculated on the basis of the Processor's hourly rates and expenses incurred for external assistance, including from sub-data processors or advisors.

IV.3 EU Standard Contractual Clauses for transfer of personal data to third countries

Before the Controller is transferring (including by access rights) personal data protected under the GDPR into a third country not recognized by the European Commission under an adequacy decision using services from Zensai provided by the Processor, the Controller represents, covenants, and warrants that the Controller and its counterpart have adopted the EU Standard Contractual Clauses ("SCC") for transfer of personal data, either as a data importer or a data exporter, respectively, in order to provide privacy rights under the GDPR for such personal data as uploaded, posted, delivered, provided or otherwise transmitted or stored into the Service and made available to users.

The Processor represents, covenants, and warrants that the Processor, as a data exporter, and its affiliates in US (Zensai US Inc.) & Australia (Zensai ANZ Pty Ltd) as a data importer, in respect to the GDPR, have adopted SCC covering delegations to respectively Zensai US Inc. & Zensai ANZ Pty Ltd for participating in providing services offered to the Controller and, incidental to these services, access and process personal data within services provided by Zensai.

APPENDICES – FOR TRANSFERS TO THIRDS COUNTRIES

Appendix 1 EU Commission SCC Module 4: Processor to Controller

Download and review via Zensai DPA-page here.

Appendix 2 UK Transfer Addendum to the EU SCC

Download and review via Zensai DPA-page here.

Appendix 3 Swiss Adaption to the EU SCC

Download and review via Zensai DPA-page here.