# Zensai Data Processing Agreement

**Between :**

**Data-controller/customer:**

Name ______________________________
Address ______________________________
Postcode and city ______________________________
Country ______________________________

("Customer" or the "controller"

**Data-processor/company:**

**Zensai International ApS**
Reg.no CVR 32139728
Mariane Thomsens Gade 4B – 5,
8000 Aarhus C,
Denmark,

("Zensai" or the "processor")

as detailed in the Order Form for subscription to Zensai Services under the Zensai Software as a Service Agreement

(also individually named a "Party" and collectively the "Parties")

have agreed on the Zensai Data Processing Agreement in order to meet the requirements of the GDPR and other applicable Data Protection Legislation to ensure the protection of the rights of the data subject.

The Zensai Data Processing Agreement consist of this main agreement and the following Annexes and Appendices:

**Annexes**

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

# SECTION I

*Clause 1*

## *Purpose and scope*

(a) Zensai Data Processing Agreement (the "DPA") is incorporated into and made part of the Zensai Software as a Service Terms (https://zensai.com/saas-terms/) and related Order Forms referencing this DPA (collectively the "Agreement"). The DPA governs the processing of personal data in connection with the Zensai services (the "Services") performed under the Agreement and sets out the terms for the data processing.

(b) The DPA is based on and integrates the terms of the EU Standard contractual clauses for controllers and processors in the EU/EEA adopted by the EU Commission under article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or "GDPR").

(c) 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.

(d) Zensai is a Danish company operating within the EU and, therefore, 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.

(e) 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. Other entities defined as controllers and processors listed in Annex I have agreed to the DPA in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679. 1. 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*) and Annex 1.

(f) 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. "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.

(g) Where Zensai is processing personal data as a controller, the Zensai Privacy Policy shall apply to such processing and not this DPA.

(h) 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.

(i) 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.

### *Clause 2*

### ***Invariability of the DPA***

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

(b) 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

### *Clause 3*

### ***Interpretation***

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

(b) The terms of the DPA shall be read and interpreted in the light of the provisions of the GDPR. Referrences to ”Member States” shall include all EEA Member States.

(c) 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.

### *Clause 4*

### ***Hierarchy***

(a) The DPA supplements and amends and forms part of the Agreement.

(b) 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.

(c) 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.

*Clause 5*

### ***Docking clause***

(a) 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 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 the DPA 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 the DPA 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.

*Clause7*

### ***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 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.

(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 EU 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 and Annex IV.

### 7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex IV 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 the DPA.

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

(c) 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.

(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 the DPA, including the results of any audits, available to the competent supervisory authority/ies on request.

### 7.3. Duration of the processing of personal data

(a) 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.

(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 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.

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

### *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 the 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 obligations in Article 32 of the GDPR.

(d) The Parties shall set out in Annex IV 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 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:

(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 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.

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 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:

(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 IV 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.

## SECTION III – FINAL PROVISIONS

*Clause 10*

### *Non-compliance with the DPA and termination*

(a) 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.

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

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with the DPA 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 the DPA or its obligations under the 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 the DPA or to the GDPR.

(c) 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 (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 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.

*Clause 11*

### *Governing Law and Venue*

(a) The DPA with its Annexes and Appendices is governed by Danish laws and shall be construed and enforced in accordance with these laws, including the GDPR which takes direct effect in Danish Law, however, without giving effect to the Danish conflict of law rules to the extent that such rules are non-mandatory.

(b) The venue shall be the courts of Denmark when dispute resolution before a court in an EU Member State is required under the GDPR, the Data Protection Legislation, or under this DPA, including the Appendices in form of the EU SCC.

(c) Disputes between the Parties, not subject to Clause 11(b), arising out of this DPA or related to the subject matter of privacy as regulated by this DPA, shall be finally settled by arbitration administered by the Danish Institute of Arbitration in accordance with its Rules of Arbitration in force at the time when such proceedings are commenced. The arbitral tribunal shall consist of three (3) arbitrators. The arbitration shall take place in Copenhagen, Denmark, and shall in all aspects be treated as confidential. The arbitration shall be conducted in the English language unless the Parties agree otherwise. The award of the arbitrators shall be final and binding on both Parties. The Parties may agree on another venue for resolving an identified current dispute. Such agreement must be made in writing and signed by both Parties and cannot include a general deviation of governing venue a stated in this Clause 11(b) and (c).

(d) The DPA shall take priority over any similar provisions contained in other parts of the Agreement between the Parties and according hereto, any conflict between the terms of the DPA and the SaaS Agreement shall be resolved in favor of the DPA.

## *Clause 12*

### ***Commencement and termination***

(a) The DPA shall come into effect on the date of concluding the Agreement.

(b) 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.

(c) 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.

(d) If the Services under the Agreement is terminated, and the personal data is deleted or returned to the controller pursuant to Clause 10(d) and Annex IV.4., the DPA may be terminated by written notice by either Party.

## ANNEX I LIST OF PARTIES

## Controller:

Company: ______________________________
Address: ______________________________

### Controller contact person 1:

Name ______________________________
Position ______________________________
Contact details ______________________________

Signature and date: ___________________________

### Controller contact person 2:

Name ______________________________
Position ______________________________
Contact details ______________________________

Signature and date: ___________________________

## Processor:

Name: Zensai International ApS
Address: Mariane Thomsens Gade 4B 5; DK-8000 Aarhus C; Denmark

### Processor contact person:

Name ______________________________
Position ______________________________
Contact details dataprotection@zensai.com

Signature and date: ___________________________

### Acceding Parties to the DPA

An affiliate of the processor (an "acceding affiliate") may accede as a party to the DPA under the terms of Section II, Clause 5 (*the Docking Clause*) when processing activities as instructed under the DPA have been agreed in a contract between the controller and the acceding affiliate (a "Contract").

The Contract must refer to and integrate the DPA and must be approved by the processor Zensai International ApS. Upon signing the Contract, the acceding affiliate shall then become a party to the DPA and have the rights and obligations of a processor under the

DPA. The acceding affiliate shall have no rights or obligations arising under the DPA from the period prior to becoming a party to the DPA.

For any additional personal data to be processes and/or data processing activities to be performed under the DPA, the data controller and the acceding affiliate shall add a description thereof to this ANNEX 1, which must be accepted by the processor Zensai International ApS, before accepted as a processing activity under the DPA.

**Affiliates of Zensai International ApS**

Zensai Deutschland GmbH
Reg. no DE342906207
Alte Papierfabrik 26
40699 Erkrath, GERMANY

Zensai US
5940 S. Rainbow Blvd,
Suite 400 #33529
89118 Las Vegas, Nevada
USA

Zensai Poland Sp. Z.o.o
Reg. no 524804402
ul. TOWAROWA, nr 28
00-839 Warszawa
POLAND

Zensai ANZ Pty Ltd
Reg. no ABN 40 142 331 002
Level 21, 8 Chifley Square
2000 Sydney, NSW
AUSTRALIA

Zensai UKI LtD
Reg. no 08225904
4 Ellice Way
Wrexham Technology Park
LL13 7YT Wrexham
Wales, United Kingdom

## ANNEX II: DESCRIPTION OF THE PROCESSING

### II.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, cf. the DPA, Clause 1(2) 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.

### II.2 The nature of the processing:

Zensai will as 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 C

### II.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.

### II.4 Categories of personal data processed

#### II.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.

### II.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.

## II.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 IV.4.

## ANNEX III: LIST OF SUB-PROCESSORS

### III.1 Approved sub-processors

The controller shall, on the commencement of the Services, authorise the use of the sub-processors which the processor may apply for processing the Services ordered.

The processor has the data controller’s general authorisation for the engagement of sub-processors following the procedure stated in the DPA, Section II, Clause 7.3.

### III.1.1 List of approved sub-processors

On commencement of the Services, the controller authorises the engagement of the following sub-processors:

| NAME | COUNTRY/REGION | PURPOSE | TYPES OF PERSONAL DATA PROCESSED | DURATION |
|---|---|---|---|---|
| **Microsoft** | For Learn365 Services, the data controller chooses relevant data centre. Updated list of data centres can be found here: Data Center Locations and Physical Security – Trust Center (zensai.com)<br>For transitional period until end 2024 - Perform365 & Engage365 data are stored in Microsoft Datacenter in UK South. | Services  is operated on the Microsoft Azure cloud platform services. Azure data centres are used for all processing activities incl. hosting of application, data and backup. | See Referenced in Annex **II.4**<br>For supplementary measures implemented see Annex IV.2 on Data security and encryption | During the term of the Service and until end of the retention period cf. Annex IV.4 |
| **Zendesk** | Dublin, Ireland | Help desk application. | Contact information, first name, last name, company email address. | During the term of the Service and until end of the retention period cf. Annex IV.4 |

### III.1.2 Feature specific Sub Processors

When the controller subscribes for additional services of the data processor, the controller authorises the engagement of the following sub-processors:

| NAME | COUNTRY/REGION | PURPOSE | TYPES OF PERSONAL PROCESSED | DURATION |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **GO1** | GO1 | Standard – Microsoft Azure Datacenter in Sydney, Australia; at request Microsoft Azure Datacenter in Dublin, Ireland can be selected.<br>Go1 \| Transformational Learning through Online Courses | Consumption of GO1 content material operated on Microsoft Azure Platform | First-name, last-name, email-address, IP-address (IP address is always stored in Microsoft Azure Data Center in Sydney, Australia) |
| **Microsoft** | For all AI-services Micosoft Open AI-datacenters depending on the region location of customer – EU/Switzerland/North Americas.<br>Updated list of data centres can be found here:<br>Data Center Locations and Physical Security – Trust Center (zensai.com) | AI based Services offered as a feature to Learn365, Perform365 & Engage365 operated on the Microsoft Azure cloud platform services.<br>See AI Product-overview here :<br>Zensai and Artificial Intelligence (AI): data, privacy, and security – Trust Center | See Referenced in section **II.4**<br>For supplementary measures implemented see Annex IV.2 on Data security and encryption | When activated as a feature by the controller, during the term of the Service and until deactivated by the controller or at the end of the retention period cf. Annex IV.4 |
| **Merge.dev** | Merge.dev are providing integration services via Amazon Web Services (AWS). When enabling Integrate365; then customer can choose datacenter within US (Virginia), EU (Stockholm) or APAC (Singapore).<br>Merge.dev – Trustcenter: here<br>Security : here. | Integrate365 – product to integrate to Human Resources Information Systems (HRIS). | Integrate365 will include these data – as minimum :<br>• Title<br>• Name<br>• Email<br>• Manager<br>• **Profile data:**<br>○ Department<br>○ Job title<br>○ City<br>○ Office<br>○ Country<br>○ Company<br>Dependant on customer needs data this can be extended to more data. | During the term of the Service and until end of the retention period cf. Annex IV.4 |

III.1.3 The processor provides installation and other support services to the data controller using its affiliates as sub-suppliers, including for 24/7 support and local services ("Purpose"). For this Purpose, and if the controller admits access to encrypted data, the affiliates may become sub-processors and have access to personal data as referenced in section **II.4**

| NAME | CITY/AREA -COUNTRY |
|---|---|
| **Zensai Deutschland GmbH** | Erkrath, Germany |
| **Zensai US** | Las Vegas, USA |
| **Zensai Poland Sp. Z.o.o** | Warszawa, Poland |
| **Zensai ANZ Pty Ltd** | Sydney, Australia |
| **Zensai UKI Ltd** | London, United Kingdom |

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

## IV.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 IV.

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

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.

## IV.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 is developing its products according to "best practices" and use of secure development procedures:

Secure Development Lifecycle (SDLC) – Trust Center (zensai.com)

The processor shall apply, and ensure that its sub-processors comply with the following minimum-security requirements:

### Availability

The processor leverages the Microsoft Azure cloud platform and implements applicable and recommended security features available on Microsoft Azure.

As such, the processor has security features in place including, but not limited to, firewall, DDOS protection, antimalware protection, anomaly detection on server behaviour and antivirus.

Further, the processor has access restrictions implemented throughout the platform in terms of authenticating both users and applications access to services which interact with data.

The processor monitors every service and has alarm systems in place if anything out of the ordinary occurs. Also, the processor continuously evaluates the measures in place based on the implemented Information Security Policy.

## Integrity

Every application in the processor's services has logging services implemented which record all operations on the data.

Logging services have both audit logs and application logs which log historical events.

Further access to manipulating data is restricted to specific user roles and hence governed by managed access in the form of both implemented systems and organisational structures, preventing unintended and/or malicious or accidental access to data.

Being a multitenant environment and SaaS, the processor's data architecture ensures the integrity and isolation of the controller’s data by separating data logically based on universally unique identifiers (UUIDs) so customer data is separated logically and secured from other customers. Customers, therefore, share the cloud platform and application, but each tenant’s data is isolated and remains invisible to other tenants.

## Confidentiality

The processor leverages different technologies in terms of securing data, depending on the nature of the data. All databases are encrypted. Data stored in databases is further encrypted using industry-standard encryption algorithms.

Extremely sensitive data such as secrets and credentials are secured by an encryption service using Microsoft Azure Key Vault.

The processor has included terms of confidentiality in the agreements with all employees, suppliers and SubProcessors. All employees are required to use two-factor authentication and strong passwords that are unique from other services.

Furthermore, the processor maintains automatic access and security logs in multiple locations.

Personal data access is governed by the processor’s documented security policies and limited to a small set of employees as required for support and maintenance. Access is further limited to a small whitelist of IP addresses via VPN and requires public key authentication.

Individual employee access follows a principle of least access. Access rights are reviewed quarterly.

## Thrustworthy AI

The processer only applies trustworthy AI systems. The standard of trustworthiness requires, that all AI tools in any form, throughout their entire life cycle must qualify as lawful, ethical, and robust:

- ***Lawful*** means complying with applicable laws and regulations;
- ***Ethical*** means ensuring adherence to ethical principles and values; and

- ***Robust*** means not causing any unintentional harm, but perform in a safe, secure, and reliable manner, both from a technical and social perspective.

A risk assessment is made for the AI on an ongoing basis throughout the lifecycle of the AI systems applied by the processer. The risk assessment identifies potential risks and evaluate, document, and communicate the the processor's evaluations made based on the proportionality of risk compared to the benefits of the application of the AI System, the trade-offs made, and describe supplementary measures taken, including for minimization and reporting of negative impacts.

For AI-services provided through Microsoft Azure Open AI-services – Data, Privacy and Security is described via this article :

Data, privacy, and security for Azure OpenAI Service - Azure AI services | Microsoft Learn

**Data security and encryption:**

Data at rest:

*Database encryption*
Azure SQL Transparent Data Encryption (TDE)* helps protect the Azure SQL server and database(s) against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups and transaction log files at rest. Each database page is decrypted when read into memory and then encrypted before being written to disk. Hence, data is never written to disk without first being encrypted.

*all services use TDE with a customer-managed key (BYOK) stored and managed securely within an Azure Key Vault within the Azure data region selected by the data controller while installing services. For further information, please visit: Transparent data encryption - Azure SQL Database & Azure SQL Managed Instance & Azure Synapse Analytics | Microsoft Learn

*Storage data (large file storage)*
Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. All Azure Storage resources are encrypted, including blobs, disks, files, queues and tables. All object metadata is also encrypted.
For further information, please visit: Azure Storage encryption for data at rest | Microsoft Docs.

Data in transit

Transmission of data between the application and Azure is secured using an encrypted TLS 1.2+ connection with AES encryption. SSL/TLS certificates are signed by a publicly known Certificate Authority using the SHA256 with a 2048 bit key.

Cookies containing session information and other sensitive data from the services are all configured with HttpOnly and Secure flags enabled. This protects the cookie contents from being accessed by scripting as well as from being transmitted over unencrypted connections.

Furthermore, the services domain is included in the HTTP Strict Transport Security (HSTS) preload list of all major browsers, meaning that these browsers will never connect to the services without an encrypted connection.

**Portability**

The Services supports export of data in Excel, ZIP & JSON formats using built-in Export actions or via Cloud API for each service

**Resilience of systems**

The Services is built entirely using Azure's platform as a service component, all operated securely in the Microsoft Azure cloud fully managed by data processor. Maintenance and updates are included in the subscription to the Services.

Each customer can select which Azure data centre they would like to use for data location upon the first installation. The options are:

Data Center Locations and Physical Security – Trust Center (zensai.com)

**Azure facilities, premises and physical security**

The processor does not have any in-house data centres, physical networks and/or servers connected to the services. Microsoft manages the physical and environmental security of our Azure-based data centres. The Azure physical security is described here and in Platforms and Standards:

Advanced Platform Security & Threat Protection – Trust Center (zensai.com)

The processor's internal security program covers physical security at our offices.

**Data breach detection and notification**

How the processor detects and responds to a breach of personal data, and notifies the controller under the GDPR

All Services and personnel follow internal incident management procedures to ensure that proper precautions are taken to avoid data breaches in the first place. In addition all Zensai services and Microsoft's Azure cloud services have specific security controls in place across all services & platforms to detect data breaches in the rare event that they occur.

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 24 hours after becoming aware of the breach, notify the controller in writing and, additionally, in any other reasonable and prompt manner (e.g. by phone or email).

In the event of a security breach, the processor's security team will promptly notify the controller of any occurrence of unauthorised access to its data. Service availability incidents are published to status page at status.zensai.com with additional information.

Should the controller’s security team need additional logs for their investigation of an incident determined to affect its organisation, the processor’s security team will coordinate and provide access as needed.

The breach notification will contain at least the following:

- A description of the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned.
- The name and contact details of the person responsible for the processor’s data protection matters.
- A description of likely consequences and/or realised consequences of the breach.
- A description of the measures taken to address the breach and to mitigate its possible adverse effects.

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. After having notified the controller in accordance with the above, the processor will, in consultation with the controller, take appropriate measures to secure the data and limit any possible detrimental effect to the data subjects.

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 ervices, to establish root causes and remediation steps, to preserve evidence and to mitigate any damage caused to data subjects or the controller.

**Data backup, retention and media sanitation**

The processor stores all data securely with full redundancy on Microsoft Azure. Each customer has their own dedicated Azure SQL Database with data and backups encrypted with Transparent Data Encryption (TDE) - see Data Security and Encryption.

All database backups are managed automatically by Microsoft Azure and are backed up as follows:

| | |
|---|---|
| Full backups | Weekly |
| Differential | Every few hours |
| Transaction log | Every 5 - 10 minutes |
| Retention | 35 days |

Note that database backups will be geo-replicated to the paired region.

For further information please visit Automatic, geo-redundant backups - Azure SQL Database & Azure SQL Managed Instance | Microsoft Docs.

**Physical security of locations at which personal data is processed**

The processor's Information Security Policy contains specific controls, rules, and guidelines regarding the locations at which personal data is processed, such as a password policy, rules of the password manager and enforcement of two-factor authentication.

Servers used by the processor belong to Microsoft, where main access to the data centre facilities are typically restricted to a single point of entry that is manned by security personnel. The main interior or reception areas have electronic card access control devices on the perimeter door(s), which restrict access to the interior facilities. Rooms within the Microsoft data centres that contain critical systems (servers, generators, electrical panels, network equipment etc.) are restricted through various security mechanisms, such as electronic card access control, keyed lock on each individual door, man traps and/or biometric devices.

### Requirements for the use of home/remote working

The processor's employees are instructed in appropriate technical and organisational measures in order to uphold Confidentiality, Integrity and Availability (CIA) principles at the processor office, and when remote working.

### Requirements for logging

The processor uses Azure policies to ensure that all Azure resources are collecting the correct security and audit logs according to the Microsoft Azure ISO 27001Regulatory Compliance standards.

For log management and review, the processor has implemented Azure Sentinel. Azure Sentinel is a cloud-native Security Information and Event Management (SIEM) system that analyses all security and audit logging data in real time using cloud based compute power and artificial intelligence for automated investigation and response (AIR). These capabilities enable security operations centre to operate more efficiently and effectively 24/7.

## IV.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, Section II, Clause 8 by implementing the following technical and organisational measures:

Assistance to the controller is provided by implementing a suitable set of standards and controls, including policies, processes, communication channels, procedures, organisational structures, software and hardware systems, that enable the processor to provide the right level of assistance to the controller. These controls and standards are established, implemented, monitored, reviewed and improved where necessary to ensure that the specific security and compliance objectives, as well as the purposes of the data protection law GDPR, are met.

The processor has defined and implemented a policy for information security and privacy and will, for personal data, maintain the following technical and organisational measures to assist the controller:

### Organisation of Information Security, risk assessment and treatment

### Appointed responsible for Information Security and assistance to the controller

The processor, has appointed a responsible for delegating, coordinating and monitoring the security rules and procedures.

### Information Security Policy

An information security policy governing how data processing, protection and privacy of personal data is ensured in compliance with relevant legislation, regulations and as required in the processor Information Security Policy, and to ensure assistance to the controller with compliance for exercising the data subjects' rights, assistance to the controller in relation to audits and inspections, and assistance to the controller in relation to ensuring compliance with the obligations pursuant to Articles 32 – 36, are implemented.

### Security roles and responsibilities

The processor's personnel with access to personal data are subject to confidentiality obligations.

### Risk management

The processor performs a risk assessment on processing activities before processing the personal data or launching new modules, components and features as part of  Zensai's Services and Platforms

The processor retains its security documents pursuant to its retention requirements after they are no longer in effect.

The processor's Information Security Policy may be sent to the controller on request.

### Asset management

*Asset inventory*

All critical assets required for running the business are identified, have an owner and are documented in a register that is kept up-to-date by the pointed-out employer.

*Asset handling*

The processor classifies personal data to help identify it and to allow for access to it to be appropriately restricted.

The processor's personnel must obtain authorisation prior to storing personal data on portable devices or remotely accessing personal data.

### Human resources security

*Security training, education and awareness*

The processor informs its personnel about relevant security procedures and their respective roles. The processor also informs its personnel of possible consequences of breaching the security rules and procedures. The processor will only use anonymous data in training.

### Physical and environmental security

*Access to processing physical processing activities*

The processor's personnel and authorised and approved third party users protect assets from unauthorised access, disclosure, modification, destruction or interference.

*Physical access to components*
The processor's personnel have no physical access to physical components nor data centres for processing activities since the processor's Services and Platforms is hosted on a cloud platform.

*Component disposal*
The processor controls that vendors use industry standard processes to delete personal data when it is no longer needed.

**Communications and operations management**

*Operational policy*
The processor maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to personal data.

*Data recovery procedures*
Backups are made continuously of all critical data and software, and everything is stored in the cloud by approved cloud vendors (sub-processors):

- On an ongoing basis, to a specific point in time within 35 days for all Zensai-services, data processor maintains a full backup of personal data from which personal data can be recovered;

- Monitoring of data recovery procedures are in place to timely detect and correct errors in the backup process;

- In case of a disruption recovery, procedures are defined in an internal process for incident management;

- The processor has specific procedures in place for governing access to copies of personal data. The processor ensures backups are not corrupt and can be used to restore data;

- The processor reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services, which are reviewed every twelve months; and

- The processor logs data restoration efforts, including the person responsible, the description of the restored data and, where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

*Malicious software*
The processor has anti-malware controls to help avoid malicious software gaining unauthorised access to personal data, including malicious software originating from public networks.

*Encryption*

All personal data is encrypted and protected against physical or digital theft of the raw data. This implies all data is encrypted . Further some data is  encrypted and/or inaccessible by unauthorised access such as the processor’s personnel who are not required to see the data in its raw format.

*Application and event logging*
All applications and/or services are designed to log their internal behaviour with respects to understanding failures and daily operation. Any application and/or service that deals with sensitive information is designed to keep an audit log which allows for complete auditing of the service. The log format is designed to be viewable in a way which does not compromise data security in terms of sensitive information.

*Data deletion*
Data is continuously deleted after the respective retention period has ended or upon request by the data controller.

**Access control**

*Access policy*
The processor maintains a record of security privileges of individuals that have access to personal data.

*Access authorisation*

- The processor maintains and updates a record of personnel authorised to access data processor’s systems that contain personal data;
- The processor deactivates authentication credentials that have not been used for a period of time not to exceed six months;
- The processor identifies those personnel who may grant, alter or cancel authorised access to personal data and resources; and
- The processor ensures that where more than one individual have access to systems containing personal data, the individuals have separate identifiers/log-ins.

*Least privilege*

- Technical support personnel are only permitted to have access to personal data when needed
- The processor restricts access to personal data to only those individuals who require such access to perform their job function.

*Integrity and confidentiality*

- The processor instructs its personnel to disable administrative sessions when computers are otherwise left unattended
- The processor stores passwords in a way that makes them unintelligible while they are in force.

*Authentication*

- The processor uses industry standard practices to identify and authenticate users who attempt to access information systems with personal data

- Where authentication mechanisms are based on passwords, the processor requires use of strong passwords of at least eight characters, in accordance with our password policy
- The processor enforces use of multi-factor authentication for all user accounts
- The processor ensures that deactivated or expired identifiers are not granted to other individuals
- The processor uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed and during storage.

**Business continuity management**

The processor maintains emergency and contingency plans for the facilities and the devices in which the processor access and process personal data. The processor's contingency plan is tested at least once a year.

The processor redundant storage and its procedures for recovering personal data are designed to attempt to reconstruct personal data in its original or last-replicated state from before the time it was lost or destroyed.

### IV.4 Storage period / erasure procedures

*What happens to the data when the controller terminates the Service?*
It is the processor's responsibility to permanently destroy the controller's data upon the data controller's request, with special emphasis on destroying all data in the scope in all locations and ensure all copies have been discarded.

The processor shall at its own discretion determine data destruction schedules but shall wherever possible perform such destruction in accordance with the controller's requested timetable. The processor shall have the obligation to wipe persistent media used for storing the controller's data or secure deletion of the controller's data with related techniques before it is released into re-use.

*Data deletion and retention period*
When the service subscription ends, the controller's data will be deleted after 90 days from the Microsoft Azure Subscription. The data will still be available on the backup to a maximum of 35 days after which time the data will be completely unobtainable. This Data Processing Agreement will continue to apply during the continued storage of the controller's data.

*Data deletion on physical storage devices on Azure*
Due to all services provided via Zensai is being built on Microsoft Azure as SaaS solutions, the processor does not have physical access to wipe and destroy media used for storing the controller's data on Azure. The media used for storing the data on Azure follows Microsoft Media Sanitation guidelines below.

If a disk drive used for storage suffers a hardware failure, it is securely erased or destroyed before Microsoft returns it to the manufacturer for replacement or repair. The data on the drive is completely overwritten to ensure the data cannot be recovered by any means.

When such devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation.

Microsoft is governed by strict standards and removes cloud customer data from systems under our control, overwriting storage resources before reuse, and purging or destroying decommissioned hardware.

Within Learn365-service course catalogues (SharePoint site collections), courses (subsites of the site collections) and content within these (objects stored - e.g., word documents, PDFs etc.) following apply:

These sites and their content belong entirely to the client's Microsoft 365 tenant and, therefore, the processor does not delete these sites or their content.

Upon termination of the Services with the personal data processing activities, the processor shall either delete or return the personal data in accordance with the DPA, Section II, Clause 10(d), unless the controller – after adopting the DPA – has modified the controller's original choice. Such modification shall be documented and kept in writing, including electronically, together with the DPA.

### IV.5 Processing location

Processing of the personal data under the DPA cannot be performed at other locations than the following without the controller's prior written authorisation.

Please see table in this Annex IV.2., locations of data processing.

### IV.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-data processors listed in Annex III.

The processor uses the EU Commission's Standard Contractual Clauses as a basis for transfer of personal data to third countries and, upon an assessment of risk, appropriate supplementary measures.

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.

### IV.7 Procedures for the controller's audits, including inspections, of the processing of personal data being performed by the processor

The processor shall once a year obtain an ISO 27001 & ISO 27701 certification report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

The Parties have agreed that the following types of certification report may be used in compliance with the DPA:

ISO 27001 certification report
ISO 27701 certification report

Based on the results of such an audit/inspection, the controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

The controller or its representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the controller deems it required.

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

The Parties acknowledge that the processor uses external auditors to verify the adequacy of its security measures.

The audit:
(i) Will be performed at least annually
(ii) Will be performed according to ISO 27001 & ISO 27701 standards or such other alternative standards that are substantially equivalent to ISO 27001 & ISO 27701
(iii) Will be performed by independent third party security professionals at the processor's selection and expense.

At the controller's written request and without charge, the processor will provide the controller with a confidential summary of the report ("Summary Report") so the controller can reasonably verify the processor's compliance with the security and audit obligations under this DPA. The Summary Report will constitute the processor's confidential information under the confidentiality provisions of the Agreement.

## ANNEX V  ADDITIONAL TERMS OF AGREEMENT

### V.1. Documentation

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

### V.2 Assistance to the controller and extra documentation

The processor's assistance to the controller in accordance with Section II, Clause 8 and regarding "extra documentation" in Annex IV, 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.

### V.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) & Australia (Zensai ANZ Pty Ltd) as a data importer, in respect to the GDPR, have accepted and submitted to the DPA and the SCC covering delegations to respectively Zensai US & 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 2: Processor to Controller & SCC Module 4: Processor to Controller

Download and review via DPA-page on https://zensai.com/:

https://zensai.com/dpa/

### Appendix 2 UK Transfer Addendum to the EU SCC

Download and review via DPA-page on https://zensai.com/:

https://zensai.com/dpa/

### Appendix 3 Swiss Adaption to the EU SCC

Download and review via DPA-page on https://zensai.com/:

https://zensai.com/dpa/