Altis DXP Customer Subscription Terms

DATA PROCESSING ADDENDUM

This Data Processing Addendum (“DPA”) is an agreement between Provider and Customer and supplements the Customer Subscription Terms and Order Form(s) (“Agreement”). Capitalized terms not otherwise defined herein will have the meanings given to them in the Agreement.

DEFINITIONS

“Data Protection Law” means all applicable current data protection, privacy and electronic marketing legislation, including (i) the General Data Protection Regulation (EU 2016/679) (“**EU GDPR**”) and the UK GDPR, as that term is defined by section 3(10) (as supplemented by section 205(4)), of the UK Data Protection Act of 2018 (“**UK GDPR**”); and (ii) any national implementing laws (including laws implementing the Privacy and Electronic Communications Directive 2002/58/EC), and the UK Data Protection Act 2018; and (iii) any other applicable national, provincial, federal, state, and local legislation, including, without limitation, the California Consumer Privacy Act (“CCPA”), and any associated regulations and secondary legislation, as amended or updated from time to time, as applicable to either party.

“EU Standard Contractual Clauses” means the annex found in the European Commission decision of 4 June 2021 on the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, specifically Module 2 and Module 3 (as applicable), and any modifications and replacements to them, or other standard contractual clauses adopted by the European Commission and entered into by the parties, from time to time.

“GDPR” means the EU GDPR and/or UK GDPR, as applicable.

“Personal Data” means Personal Data that is uploaded to, generated by or transmitted via the Provider Solution under Customer’s Provider Solution accounts for processing as described herein.

“Standard Contractual Clauses” means the EU Standard Contractual Clauses and/or the UK Addendum, as applicable.

“Sub-processor” means any processor that is engaged by a party to assist in its processing of Personal Data for another party.

“UK Addendum” means the ICO’s UK Addendum to the EU Standard Contractual Clauses, as amended from time to time, and available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.

“controller”, **“data subject”**, **“processor”**, and **“processing”** as defined in the UK GDPR or the EU GDPR, as applicable.

DATA PROTECTION

1. Both parties will comply with all applicable requirements of the Data Protection Law. This DPA is in addition to, and does not relieve, remove, or replace, a party’s obligations under the Data Protection Law.

2. This DPA applies to Personal Data processed by Provider for Customer, if any. In this context, Provider may act as “processor” to Customer, who may act either as “controller” or “processor” (as those terms are defined in Data Protection Law) with respect to Personal Data.

3. Details of Personal Data processing (Annex 1 and Annex 2 to the EU Standard Contractual Clauses and/or Appendix Information for the UK Addendum, as applicable):

Data Exporter: the Customer, as the party sending Content, some of which may contain Personal Data, to Provider for Provider's processing in furtherance of provision of the Provider Solution.

Data Importer: Provider as a conduit of Content transmitted through the use of the Provider Solution, some of which may contain Personal Data.

Subject Matter: the subject matter of the data processing under this DPA is the data and content as described below.

Purpose: the provision of the Provider Solution initiated by Customer from time to time.

Nature of the Processing: provision of Provider Solutions as described in the Agreement and initiated by Customer from time to time.

Categories of Data Subjects: the Data Subjects may include Customer's end users, visitors, guests, employees and staff, and any others whose Personal Data is captured in Content.

Description of Processing: in addition to Personal Data incidentally captured and processed as Content in the Provider Solution ("Captured Personal Data"), Provider collects and processes the following as a necessary step in providing the Provider Solution, all or some of which may or may not be personally identifying or identifiable information:

- IP addresses
- User credentials (username, password, and MFA tokens)
- Names

- Email addresses

Content transmitted through the use of the Provider Solution may, unbeknownst to Provider, contain Personal Data. Such Captured Personal Data is held only for as long as needed to transmit it (except if and to the extent of such data the Customer elects to store, as data controller). Other Personal Data is retained for 90 days, other than IP addresses, which are stored indefinitely.

Special Categories of Data: the parties do not anticipate or knowingly enact the transfer of special categories of data.

Duration of Processing: during the term of the Customer's subscription and for 90 days thereafter.

Processing Operations: as described in this DPA, including Annex 1.

Competent Supervisory Authority: Data Protection Commissioner of Ireland (EU); Information Commissioner's Office (UK; **"ICO"**).

4. Customer will ensure and warrants that it has all necessary and appropriate consents and notices, in any form required by Data Protection Law, in place to enable lawful transfer of the Personal Data to Provider for the duration and purposes of the Agreement.

5. Customer will ensure and warrants that where Personal Data is transferred outside the European Economic Area ("EEA") or outside the UK, as part of Customer's use or deployment of the Provider Solution, adequate measures will be taken to ensure the Personal Data will be protected to an adequate level and the data subjects' rights under the Data Protection Law will not be prejudiced by such a transfer. Subject to Provider's obligation in section 9.5 below with respect to Provider sub-processors, and section 11 below with respect to the Standard Contractual Clauses if applicable, Customer acknowledges that Customer is solely responsible for ensuring that Personal Data is transferred out of the EEA or the UK in full compliance with the Data Protection Law.

6. Customer will ensure and warrants that Customer utilizes appropriate technical and organizational measures to ensure a level of security appropriate to such risks, including, as appropriate, the measures referred to in the Data Protection Law.

7. Customer confirms that it has assessed any security measures in place at the time of this Agreement, and that it will continue to do so on an ongoing basis to ensure its obligations under this DPA. Customer is solely responsible (as between the parties) if such measures fail to meet the standards required by Data Protection Law.

8. Customer undertakes and confirms that any information required to be provided to a Data Subject has been so provided or an applicable exemption is available and is being relied upon by the Customer.

9. Customer and Provider agree that to the extent each party processes any personal data of the other party's personnel in connection with entry into the Agreement or the management of their business relationship, such party processes such data as an independent controller.

10. Provider will, in relation to any Personal Data processed in connection with the provision of the Provider Solution:

10.1. process that Personal Data only on the written instructions of Customer and as set forth in the Agreement except to the extent Provider is required to process data by applicable law. Where Provider is relying on applicable law as the basis for processing Personal Data, Provider will without undue delay notify Customer unless applicable law prohibits Provider from so notifying Customer;

10.2. not access or use, or disclose to any third party, any Personal Data, except, in each case, as necessary to maintain or provide the Provider Solution, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order);

10.3. ensure that it has in place appropriate technical and organizational measures designed to protect against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures;

10.4. ensure that all Provider personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;

10.5. ensure that where Sub-processors are used outside the EEA or the UK such that Personal Data is transferred outside the EEA or the UK, and such transfer is not to a third country that the EU Commission considers to provide an adequate level of protection (in the case of transfers subject to EU GDPR) or that the UK Secretary of State considers to provide an adequate level of protection (in the case of transfers subject to UK GDPR), adequate measures will be taken to ensure the Personal Data will be protected to an adequate level (including without limitation use of the SCCs) and the Data Subjects' rights under the Data Protection Law will not be prejudiced by such a transfer;

10.6. maintain records of processing activities carried out on behalf of Customer as required by Data Protection Law;

10.7. taking into account the nature of the processing, insofar as reasonable and practicable, assist the Customer in responding to any request from a Data Subject and in ensuring compliance with its obligations under Data Protection Law with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

10.8. notify Customer without undue delay on becoming aware of a Personal Data security incident. Provider is not obligated to report unsuccessful incidents or incidents that result in no unlawful or accidental destruction, loss, alteration, disclosure of, or unauthorized access to Personal Data or any of Provider's equipment or facilities storing Personal Data. Such non-reportable incidents may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers), or similar incidents. Provider's obligation to report or respond to a security incident under this section is not and will not be construed as an acknowledgement by Provider of any fault or liability of Provider with respect to the incident; and

10.9. at the written direction of Customer, delete Personal Data to the extent Provider is capable of doing so via its standard retrieval and delete mechanism, unless required by applicable law to store the Personal Data.

11. Customer will immediately notify Provider if any necessary appropriate consents and notices required to enable lawful transfer of Personal Data to Provider for the duration and purposes of this Agreement have been breached, terminated, withdrawn, or are otherwise no longer valid.

12. The parties agree that the EU Standard Contractual Clauses apply if Personal Data subject to the EU GDPR is transferred to Provider or its sub-processors located in a third country outside of the EEA that the EU Commission does not consider to provide an adequate level of protection. The parties agree that the UK Addendum applies if Personal Data subject to the UK GDPR is transferred to Provider or its sub-processors located in a third country that is outside of the UK and that the UK Secretary of State does not consider to provide an adequate level of protection. As used in this section, the terms “Data Importer” and “Data Exporter” will have the meanings given to them in the Standard Contractual Clauses. The parties acknowledge that for the purposes of the Standard Contractual Clauses, Provider is acting in the capacity of a Data Importer and Customer is the Data Exporter (notwithstanding that Customer may be located outside of the EEA/UK or is acting as a processor on behalf of third-party controllers). Each party will comply with the applicable obligations of the Standard Contractual Clauses in their respective roles as Data Exporter and Data Importer. The data subjects, categories of data, and processing operations (as required to be disclosed in the Standard Contractual Clauses) are as set forth in this DPA. Annex 1 to this DPA details the technical and security measures Provider has implemented, as required to be disclosed in the Standard Contractual Clauses.

13. The parties further agree that the governing law of the Standard Contractual Clauses entered into by Provider and the Customer will be as follows: where the EU Standard Contractual Clauses apply and the Customer is established in the EEA, the laws of Ireland control; and where the UK Addendum applies, the laws of England and Wales control. If any inconsistency arises between this section 12 and any other provision for the governing law of the Standard Contractual Clauses entered into between Customer and Provider, this section 12 will take precedence.

14. In the event of any conflict between this DPA and the EU Standard Contractual Clauses, the EU Standard Contractual Clauses shall prevail. In the event of any conflict between this DPA and the UK Addendum, the UK Addendum shall prevail.

15. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including where applicable, the Standard Contractual Clauses) and any audit rights granted by Data Protection Law, by instructing Provider to comply with the audit measures described in Annex 1 to this DPA.

16. Provider represents and warrants that it has not received any order, request, or other communication from a governmental body for the disclosure of Personal Data and it shall:

16.1. if it receives such order, request, or other communication, attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Provider may provide Customer’s basic contact information to the relevant body. If compelled to disclose Customer Data to a governmental body, then Provider will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Provider is legally prohibited from doing so;

16.2. publish a transparency report or provide information to Customer on request regarding: (a) the number of orders, requests, or other communications from governmental bodies for the disclosure of Personal Data and/or assistance in surveillance processes and the type of information requested, (b) its responses to the foregoing, and (c) its process for challenging such confidential and non-confidential orders, requests, and communications; and

16.3. notify Customer if its ability to maintain the confidentiality and security of Personal Data has been compromised for any reason including by orders, requests or communications described above, and cease processing, including receiving such Personal Data.

17. Customer agrees that Provider may use Sub-processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services, and consents to the use of Sub-processors as described in this section. The Provider website (https://www.altis-dxp.com/policies/dpa/subprocessors/) lists Sub-processors that are currently engaged by Provider to deliver the Provider Solution. (Such webpage constitutes Annex III/Appendix 3 to the Standard Contractual Clauses if and as applicable.) At least 10 business days before Provider engages any new Sub-processor to carry out processing activities on Personal Data on behalf of Customer, Provider will endeavor to update the applicable website and provide Customer notice of that update as per the means specified for notices in the Agreement. If Customer objects to a new Sub-processor, Customer must notify Provider in writing within ten days of Customer's notice of the change (without prejudice to any termination rights Customer has under the Agreement), after which time Customer shall be deemed to have consented to the new sub-processor's appointment in the absence of any such notice. If Customer objects to a new Sub-processor, Provider may either, in its sole discretion: (a) propose an alternative Sub-processor or remain with the current Sub-processor; or (b) refrain from the use of any Sub-processor; or (c) terminate the Customer's subscription on thirty days written notice.

18. Provider may propose revisions to this DPA by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an approved code of conduct or applicable certification scheme (which will apply when replaced by attachment to this Agreement). Customer and Provider will negotiate such changes in good faith as soon as reasonably practicable.

19. The parties agree that, if any new versions or revisions to the EU Standard Contractual Clauses are approved by the European Commission, or new versions or revision of the UK Addendum are approved and published by the ICO, such that the implementation of the Standard Contractual Clauses in this DPA no longer applies or is no longer appropriate, the parties shall work together to enter into new standard contractual clauses as appropriate.

20. Where the EU SCCs apply to transfers of Personal Data governed by this DPA, the following options shall be deemed to be selected and incorporated, each clause reference in this section being a reference to a clause in the EU SCCs: (a) Clause 7 shall not apply; (b) at Clause 9, option 2 shall apply for both Module 2 and Module 3; and (c) at Clause 11, the optional redress mechanism shall not apply.

21. California Consumer Privacy Act (CCPA) Notice: as a "Provider" (as that term is defined in the CCPA), Provider will process California Personal Data that is subject to the CCPA strictly for the purpose of providing to Customer the solutions and services described in the Agreement, or as otherwise permitted by the CCPA, and shall not retain, use, or disclose such data for any other purpose.

22. Where the UK Addendum applies to transfers of Personal Data governed by this DPA, the parties agree that:

22.1. the UK Addendum shall be populated by reference to this DPA and its Annex and that any changes in formatting (including for the avoidance of doubt with respect to Part 1: Tables) will not adversely affect the validity of the DPA or the compliance with Data Protection Law of any international transfers of Personal Data made thereunder;

22.2. any formatting changes do not reduce the standard of Appropriate Safeguards (as defined in the UK Addendum) provided;

22.3. without prejudice to any of the rights and remedies under the Agreement, pursuant to Section 19 of the UK Addendum, neither party shall be entitled to terminate the UK Addendum.

Annex 1: Technical and Organizational Security Measures

DPA ANNEX 1: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES (Annex II/Appendix 2 to the Standard Contractual Clauses, and/or UK Addendum Appendix Information, if and as applicable)

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: Provider hosts its Service with AWS and/or applicable affiliates. Additionally, Provider maintains contractual relationships with vendors in order to provide the Service. Provider relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: Provider hosts its product infrastructure with multi-tenant, outsourced infrastructure provider Amazon Web Services Inc. The physical and environmental security controls are audited for SOC 2 Type II (https://aws.amazon.com/compliance/soc-faqs/) and ISO 27001 (https://aws.amazon.com/compliance/iso-27001-faqs/) compliance, among other certifications. Provider shall provide relevant certificates to Customers upon request where possible.

Authentication: Provider has implemented a uniform password policy for its customer products for customer's use and customization. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Provider's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key.

ii) Preventing Unauthorized Product Use

Provider implements industry standard access controls capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: Provider has implemented a Web Application Firewall (WAF) solution to protect internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services, including Denial of Service (DoS) attacks.

Static code analysis: Security reviews of code stored in Provider's source code repositories is performed, checking for identifiable software flaws, and known vulnerabilities.

Penetration testing: Provider maintains relationships with industry recognized penetration testing Providers for regular penetration tests, conducted on an annual basis. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of Provider's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security.

Staff: All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards. Employees are subject to background checks prior to receiving access, including criminal and sanctions checks.

b) Transmission Control

In-transit: Provider makes HTTPS encryption (also referred to as SSL or TLS) available on all web interfaces, including every one of its login interfaces. Provider's HTTPS implementation uses industry standard algorithms and certificates, and develops and deploys improvements on a continual basis.

At-rest: Provider stores user passwords following policies that follow industry standard practices for security and ensure that all passwords are never stored in plain text formats.

c) Input Control

Detection: Provider designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Provider personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Provider maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Provider will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If Provider becomes aware of unlawful access to Personal Data of data subjects, Provider may: 1) as a member of the ICO, notify the ICO and follow ICO guidelines in regards to procedure; 2) notify the affected Customers and/or data subjects of the incident if required or permitted under applicable law; 3) provide a description of the steps Provider is taking to resolve the incident; and 4) provide status updates to the Customer contact, as Provider deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Provider selects, which may include via email or telephone.