Data Processing Agreement

For Altia Service(s)

This document in its current form is published online and made available by Altia at https://legal.altiacloud.com. A.pdf, *Microsoft Word* or printed version of this document may not be current and is provided as a signed copy, by Altia, for Customer(s) seeking 'point in time' referenceability against other documents, agreements or arrangements between the Customer and Altia.

Contents

PART A

1. Introduction and General Notes

About this document. This Data Processing Agreement **("DPA")** explains how Altia process Customer Data and includes specifics relating to compliance with GDPR. Altia's DPA is applicable to ALL Agreements, Customer(s) and User(s).

Definitions, terms and interpretation. In this document, defined terms are contained within the Altia Legal Definition Schedule **("Definition Schedule")**. Words capitalised in error appearing as a Term, or where words are intentionally not defined as Term(s) but are perceived by a Party as potentially being a Term, are to be given the meaning of the word, or words, in context, as determined by what a reasonable person, having been deemed responsibly capable for reviewing commercial agreement(s), would have understood the word(s). Definitions may be inferred from the subject of the section, and where appropriate, Terms may be defined 'in line' or their acronyms introduced.

Agreement Generalisation. The Agreement in its entirety is geographically, currency and Altia Service(s) generalised, to ensure consistency in legal and commercial agreement(s). There may be clause(s), sections or reference to the Agreement and/or Agreement Supplementary Material that are not relevant to a specific Agreement between Altia and a Customer. Section Two of this document, the Agreement and each refenced Agreement Supplementary Material outlines Applicability for Party(s) to determine if the clause(s), sections or referenced Agreement Supplementary Material are in scope of the Agreement.

Document Version. This document is made current at the date published and made available at https://legal.altiacloud.com **(the "Reference Date").** The Reference Date determine(s) the Agreement entered into, which survives in perpetuity, through Order Form(s).

Altia's right to update, change or amend. Altia, from time to time, may update this document, the Agreement and Agreement Supplementary Material. If you are supplied Altia Service(s) by Altia, through an Agreement, you will be advised of changes to this Agreement or Agreement Supplementary Material through the '*Notices to Parties*' section of Altia's Master Services Agreement **("MSA")**. Archived versions of Altia's MSA and any Agreement Supplementary Material form the Agreement against the Reference Date can be found at https://legal.altiacloud.com. If there are any disputes to clause(s) of this document, the Agreement or Agreement Supplementary Material as varied from the Reference Date, you may raise a dispute as per the '*Dispute Resolution*' Section of Altia's MSA.

2. Applicability

THIS DPA IS RELEVANT WHERE THE GDPR APPLIES TO THE PROCESSING OF PERSONAL DATA IN CONNECTION WITH ALTIA PROVIDING ALTIA SERVICE(S) TO CUSTOMER(S) OR USER(S). THIS DPA, WHERE THE GDPR DOES NOT APPLY SERVES AS ALTIA'S AGREEMENT FOR DATA PROTECTION GENERALLY.

3. Definitions

Definitions in used in this Agreement are defined in Altia's Agreement Definition Schedule **(Or, "Definition Schedule")**.

4. Compliance with Laws

a) Altia will comply with all laws and regulations applicable to its provision of the Altia Service(s), including security breach notification law and data protection requirements.

b) The Parties acknowledge and agree that the Customer will act as the Data Controller in relation to the Processing of Personal Data, and Altia will act as the Data Processor, except where the Customer acts as a Processor of Personal Data, in which case, Altia is a Sub-Processor.

c) The types of personal information that are processed pursuant to the Agreement, including the subject matter, duration, nature, scope and purpose of the processing and the categories of data and individuals are set out in the Agreement, Initiating Order, and any/all subsequent Order Form(s), Attachment(s), Annexure(s) and Schedule(s).

d) When Altia acts as the Processor or Sub-Processor of Personal Data, it will process Personal Data only on documented instructions of the Customer as detailed in the Agreement, Initiating Order, and any/all subsequent Order Form(s), Attachment(s), Annexure(s) and Schedule(s). Any additional or alternate instructions must be agreed to in writing by all Parties to the Agreement.

5. Scope

Clauses in this DPA apply to all Altia Service(s) that are provided by Altia to the Customer, under the Agreement or in absence of an executed Agreement.

6. Nature of Data Processing

Altia will use and otherwise process Customer Data and Personal Data only:

a) To provide the Customer the Altia Services in accordance with the Customer's documented instructions as detailed in the Agreement; and

b) For Altia's legitimate business operations, pursuant to the terms of the Agreement.

7. Processing to Provide Altia Service(s)

When providing Altia Service(s), Altia will not use or otherwise process Customer Data or Personal Data for:

a) User Profiling; or

b) Advertising or similar commercial purposes; or

c) Market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with the Customer's documented instructions.

8. Processing for Altia's Legitimate Business Operations

For purposes of this DPA, Altia's legitimate business operations consists generally (but not limited to) the following, each as incident to delivery of the Altia Service(s) to the Customer and/or User(s):

a) Billing and account management.

b) Internal reporting and modelling (including, but not limited to, forecasting; revenue; capacity planning; or service(s) strategy).

c) Combating fraud, cybercrime or cyber-attacks that may affect Altia or Altia Service(s).

d) Improving the core functionality of accessibility, privacy or energy-efficiency.

e) Financial reporting and compliance with legal obligations, subject to the limitations on disclosure.

9. Disclosure of Processed Data

a) All processing of Processed Data is subject to Altia's obligation of confidentiality under the Agreement. Altia will not disclose Processed Data except: if, as and when Customer(s) or User(s) directs; as described in this DPA; or as required by law.

b) Altia will not disclose Processed Data to a law enforcement or regulatory body unless required by law. If a law enforcement or regulatory body contacts Altia with a demand for Processed Data, Altia will attempt to redirect the law enforcement or regulatory body to request that data directly from Customer(s) or User(s). If lawfully compelled to disclose Processed Data to a law enforcement or regulatory body, where possible and only without breaching any legal or regulatory requirement, Altia will promptly notify the Customer(s) or User(s) and provide a copy of the lawful demand.

c) Altia will reject any third party request for Processed Data, unless required by law to comply with that request. Upon receipt of any other third party request for Processed Data, in absence of being compelled by law, where possible and only without breaching any legal or regulatory requirement, Altia will promptly notify Customer(s) or User(s) and if the request is valid, Altia will attempt to redirect the third party to request the data directly from the Customer(s) or User(s).

d) Altia will not provide any third party: direct, indirect, blanket, or unfettered access to Processed Data; encryption key(s), secret(s), passphrase(s), password(s), or programmatic access to physical or virtual storage used to secure Processed Data, or the ability to break such encryption and security measures; and/or access to Processed Data if Altia is aware that the data is to be used for purposes other than those stated in the third party's request; even if required by law, founded on fraudulent, corrupt, false or misleading grounds.

e) In support of attempts to redirect third party requests to Processed Data directly to the Customer(s) or User(s); Altia may provide the Customer(s) or User(s) basic contact information to the third party; limited to first name, surname, telephone number and/or email address.

10. Processing of Personal Data - GDPR

a) To the extent Altia is a Processor or Sub-Processor of Personal Data subject to the GDPR, the GDPR Terms in **PART B** below govern that processing and the Parties also agree to the following terms in this clause.

b) Personal Data processed by Altia in connection with Altia Services is obtained as either Customer Data, Diagnostic Data or Service Generated Data. Personal Data provided to Altia by, or on behalf of the Customer through use of the Altia Services is also Customer Data. Pseudonymised through Pseudonymisation identifiers may be included in Diagnostic Data or Service Generated Data and are also Personal Data. Any Personal Data having been Pseudonymised, or de-identified but not anonymised, or Personal Data derived from Personal Data is also Personal Data.

11. Data Security

Detailed information relating to information and cybersecurity for Altia Service(s), including the shared responsibilities of Altia, Customer(s) and User(s) is included in Altia's Shared Information and Cybersecurity Framework Schedule, which forms part of the Agreement; and can be found here. For GDPR, Customer Data and Personal Data security only, the data security clauses in this section of the DPA take priority over the inclusions of Altia's Shared Information and Cybersecurity Framework Schedule.

11.1. Security Practices and Policies

Altia has implemented and maintains appropriate technical and organisational measures to protect Customer Data and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, Personal Data transmitted, stored or otherwise processed. Controls and security models for Altia Service(s) and Altia's internal security programs & polices may be made available to Customer(s) under nondisclosure agreement upon a heavily justified written request. Altia reserve the right not to disclose, or control disclosure of internal security program, policy information and Altia Service(s) control and security models, to protect the overall security posture of Altia and the Altia Service(s).

11.2. Customer(s) and User(s) Responsibilities

a) Customer(s) and User(s) are solely responsible for making an independent determination as to if the technical and organisational measures for the Altia Service(s) meet the Customer's requirements, including any of its

security obligations under applicable data protection, or its or their jurisdiction's specific requirements.

b) Customer(s) and User(s) acknowledge and agree that, in taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals, the security practices and policies implemented and maintained by Altia provide a level of security appropriate to the risk with respect to its Personal Data.

c) Customer(s) are responsible for implementing and maintaining its or their own privacy protections and security measures for components that Customer(s) provide or control, such as devices, including Bring Your Own Device **(Or, "BYOD")** devices of User(s), accessing Altia Service(s), or within other Customer(s) System or Hardware components. User(s) are also responsible for implementing and maintaining its or their own privacy protections and security measures for component such as devices accessing Altia Service(s).

11.3. Auditing Compliance

Altia will conduct audits of the security of the computers, computing environment, physical data centres that it may use in processing Customer Data and Personal Data, as follows:

a) Where a standard or framework provides for audits, Altia will make aspirational efforts to conduct an audit of such control standard or framework annually.

b) Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.

c) Each audit will be performed by qualified, independent, third party security auditors at Altia's selection, expense and from time to time, Altia will adopt and observe well-known worldwide programs with government oversight or endorsement.

d) Each audit resulting in the generation of an audit report will be Altia's Confidential Information, and Altia will clearly disclose any material findings by the auditor to any affected Customer(s) or User(s). Altia will remediate issues raised in any audit report to the satisfaction of the auditor, where possible or adopt mitigating controls. If Customer(s) or User(s) reasonably requests (and only in circumstances where the findings of any audit report are materially detrimental to a Customer(s) use of the Altia Service(s), Altia

may provide Customer(s) or User(s) with sufficient information for the Customer(s) or User(s) to assist in remediation of any risk to them.

11.4. Security Incident Notification

If Altia becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Customer Data or Personal Data while processed by Altia, Customer(s) or User(s), Altia will promptly and without undue delay, through SIRT or PSIRT capabilities:

a) Notify the Customer of the Security Incident.

b) Investigate the Security Incident and provide affected Customer(s) or User(s) with detailed information about the Security Incident.

c) Take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident.

d) Notification(s) of Security Incidents will be delivered to affected Customer(s) or User(s) security representative, if known, by any means Altia selects, including email.

e) It is a Customer(s) or User(s) responsibility to ensure management and administrators maintain accurate contact information for notification purposes. Customer(s) and User(s) are solely responsible for complying with its and their obligations under incident notification Mandatory Notifiable Data Breach laws as and if applicable to the Customer(s) and User(s), fulfilling any third party notification obligations related to any Security Incident applicable. Customer(s) and User(s) must notify Altia promptly of any possible misuse of its accounts or authentication credentials or any Security Incident related to the Altia Service(s) known to the Customer(s) and User(s). Altia shall make reasonable efforts to assist Customer(s) and User(s) in fulfilling the obligation under GDPR Article 33, or other applicable law or regulation to notify the relevant supervisory authority and data subjects about a Security Incident.

f) Altia's notification of or response to a Security Incident under this section clause is not an acknowledgment by Altia of any fault or liability with respect to the Security Incident.

12. Data Transfers and Location

12.1. Data Transfers

a) Except as described elsewhere in this DPA or made explicit in the Agreement, Initiating Order or subsequent Order Form(s); Customer Data

and Personal Data that Altia processes on a Customer(s) or User(s) behalf may be transferred to, and stored and processed in, any country in which Altia operates and in which Third Party Service Providers, as Sub-Processors, relied on by Altia operate. The Customer(s) or User(s) appoints Altia to perform any such transfer of Customer Data and Personal Data to any such country and to store and process the Customer Data and Personal Data to provide the Altia Service(s). Where the Customer(s) or User(s) requires the Customer Data and Personal Data to remain only in one location, it is the Customer(s) or User(s) obligation to advise Altia accordingly in the Initiating Order, or subsequent Order Form(s).

b) All transfers of Customer Data out of the European Union, European Economic Area and Switzerland by the Altia Service(s) shall be governed by standard contractual clauses to be entered into by Customer(s) or User(s) and Altia in the Initiating Order, or subsequent Order Form(s).

c) Altia will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention and other Processing of Personal Data from the European Economic Area and Switzerland. All transfers of Personal Data to a third country or an international organisation will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

d) Altia maintain the right to observe future legal and regulatory requirements as a result of data protection, or privacy law.

12.2. Location of Customer(s) or User(s) Data at Rest

In providing Altia Service(s), Altia will store Customer Data at rest within any country in which Altia operates and in which Third Party Service Providers (Sub-Processors) relied on by Altia operate, or in a location explicitly requested in the Initiating Order, or subsequent Order Form(s) by the Customer. Altia does not control or limit the regions from which Customer(s) or User(s) may access or move Customer Data.

13. Data Retention and Deletion

a) At all times during the Term of the Agreement, Customer(s) and User(s) will have the ability to create, read and update the Customer Data stored in and through the Altia Services, unless Altia Service(s) features or functionality places specific restrictions on this ability, by design, as advertised and accepted by Customer(s) and User(s).

b) Subject to Customer(s) or User(s) terminating use of Altia Service(s) as provided for in the MSA, and the relevant and the Terms and Conditions of

the Initiating Order, or any subsequent Order Form, Altia will retain Customer Data that remains stored in and through the Altia Service(s) in a limited function account for 90-days after expiration or termination of Agreement so that the Customer may extract the data. After the 90-day retention period ends, Altia will disable the Customer's account and delete the Customer Data and Personal Data within an additional 90-days, unless Altia is permitted or required by applicable law, or authorised under this DPA, to retain such data.

c) Some Altia Service(s) may not support retention or extraction of software provided by the Customer.

d) Altia holds no liability for the deletion of Customer Data or Personal Data, evidence or intelligence, as defined by applicable law, as described in this clause.

14. Processor Confidentiality Commitment

a) Altia will ensure that its employees engaged in the processing of Customer Data and Personal Data will: process such data only on instructions from Customer(s), User(s), or as described in this DPA; and be obligated to maintain the confidentiality and security of such data even after their engagement ends.

b) Altia shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to the Customer Data and Personal Data in accordance with applicable data protection requirements and industry standards.

15. Notice and Controls on Use of Sub-Processors

a) Altia may hire third parties to provide certain limited or ancillary services on its behalf. Customer(s) and User(s) consents to the engagement of these third parties and Altia Third Party Service Provider(s) as Sub-Processors. The above authorisations will constitute the Customer(s) and User(s) prior written consent to the subcontracting by Altia of the processing of Customer Data and Personal Data if such consent is required under the standard contractual clauses or the GDPR Terms.

b) Altia is responsible for its Sub-Processor's compliance with Altia' obligations in this DPA. When engaging any Sub-Processor(s), Altia will ensure through contractual obligation that the Sub-Processor(s) may access and use the Customer Data or Personal Data only to deliver the services Altia has retained them to provide and is prohibited from using the Customer Data

or Personal Data for any other purpose. Altia will ensure that Sub-Processor(s) are bound by written agreements that require them to provide at least the level of data protection required of Altia by the DPA.

c) From time to time, Altia may engage new Sub-Processor(s). Altia will give Customer(s) or User(s) notice of any new Sub-Processor that is engaged and that materially impacts the Altia Service(s) provided to Customer(s) or User(s), for example, where that Sub-Processor has access to Customer Data.

d) If Customer(s) or User(s) does not approve of a new Sub-Processor, then the Customer may invoke the disputes process as described in this DPA.

PART B

16. European Union GDPR Terms

Altia makes the commitments in these GDPR Terms **("GDPR Terms"),** to the Customer. These commitments are binding upon Altia with regard to the Customer regardless of the Altia Services ordered. These GDPR Terms apply to the Processing of Personal Data, within the scope of the GDPR, by Altia on behalf of the Customer. These GDPR Terms do not limit or reduce any data protection commitments that Altia makes to Customer(s) or User(s) under the Agreement. These GDPR Terms do not apply where Altia is a Data Controller of Personal Data.

17. Relevant GDPR Obligations Articles 28, 32, 33

Altia shall not engage another Processor without prior specific or general written authorisation of the Customer. In the case of general written authorisation, Altia shall inform the Customer of any intended changes concerning the addition or replacement of other processors, thereby giving the Customer the opportunity to object to such changes (Article 28(2)). Processing by Altia shall be governed by these GDPR Terms under European Union (hereafter "Union") or Member State law and are binding on Altia with regard to the Customer. The subject matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of Customer(s) or User(s) are set forth in the Agreement. In particular, Altia shall:

a) Process the Personal Data only on documented instructions from the Customer(s) or User(s), including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which Altia is subject; in such a case, Altia shall inform the Customer(s) or User(s) of that legal requirement before

processing, unless that law prohibits such information on important grounds of public interest.

b) Ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c) Take all measures required pursuant to Article 32 (Security of Processing) of the GDPR. Respect the conditions referred to in paragraphs for engaging another processor.

d) Taking into account the nature of the processing, assist Customer(s) or User(s) with appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of a Customer(s) or User(s) obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR.

e) Assist Customer(s) or User(s) in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Altia.

f) At the request of Customer(s) or User(s), delete or return all the Personal Data to the Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data.

g) Make available to Customer(s) or User(s) all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer(s) or User(s) or another auditor mandated by the Customer(s) or User(s).

Altia shall immediately inform the Customer(s) or User(s) if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions (Article 28(3)).

Where Altia engages another processor for carrying out specific processing activities on behalf of the Customer(s) or User(s), the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, Altia shall remain fully liable to Customer(s) or User(s) for the performance of that other processor's obligations (Article 28(4)).

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying

likelihood and severity for the rights and freedoms of natural persons, Customer(s) or User(s) and Altia shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) The Pseudonymisation and encryption of Personal Data.

b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

c) The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.

d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (Article 32(1)).

In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise processed (Article 32(2)).

Customer(s) or User(s) and Altia shall take steps to ensure that any natural person acting under the authority of the Customer(s) or User(s) or Altia who has access to Personal Data does not process them except on instructions from Customer(s) or User(s), unless he or she is required to do so by Union or Member State law (Article 32(4)).

Altia shall Customer(s) or User(s) without undue delay after becoming aware of a Personal Data breach (Article 33(2)). Such notification will include that information Altia, as a Processor, must provide to a Controller under Article 33(3) to the extent such information is reasonably available to Altia.

18. Disputes

Any disputes relating to this DPA, or Altia's performance against this DPA, are to be raised in writing, within a reasonable time and in sufficient detail, with sufficient evidence to legal@altiaintel.com.

Point In Time Version Control

This document was uploaded to legal.altiacloud.com at 1am on 1 July 2022, as current, by Altia's Chief Information Officer. No prior version was available or archived.

DocuSigned by:
Brice Neilson
7E80ECF8155C49C...

Brice Neilson
Chief Information Officer
Altia | info@altiaintel.com

12 August 2022 | 9:51 AM AEST