
This Data Processing Addendum (**Addendum**) forms part of the agreement for the purchase of professional services (including but not limited to valuation management, tax and rates services), software licenses, or software subscriptions, as applicable, whether governed by a Master Customer Agreement, Master License Agreement, Master Services Agreement, Software License Agreement, Engagement Letter, Quote, Order Form, or other written or electronic agreement between Customer and the relevant member of the Altus Group (**Services Agreement**). Customer and the relevant member of the Altus Group (**Service Provider**) shall together be referred to as the **Parties**.

Customer Instructions

- 1 Customer should complete the information in the signature box and sign where appropriate. The signing party must be the same Customer entity that signed the Services Agreement.
- 2 Customer must send the signed and completed Addendum to GDPR-DPA@altusgroup.com, with the appropriate customer contact details in the email.

1 Key terms

Processing Activities

This summary sets out the details of the processing of Customer Personal Data pursuant to this Addendum.

Subject Matter and Duration

Customer Personal Data will be processed in order to allow Service Provider to provide the Services. The processing shall take place for the duration of the Services Agreement, unless otherwise directed by the Customer.

Nature and Purpose

Service Provider and its Affiliates will use the Customer Personal Data to provide the Services which have been contracted by the Parties under the Services Agreement. In particular, such Personal Data will be used to provide access to the Services, to communicate with Customer and its employees, agents, or customers, and to provide the hosting, support, and professional services to Customer.

Categories of Data Subjects

Customer Personal Data relates to the following categories of data subjects:

- applicants
- employees
- contractors and agency staff
- clients (B2C)
- customers, tenants and contacts (B2B - business contact details only)
- online registered users
- members of the public

Types of Personal Data

Customer Personal Data comprises the following categories of data:

For software services and products:

- Names
- Addresses
- Telephone numbers
- Emails

- IP addresses and other similar technical information required to provide the applicable products and services.

For professional services and other services:

- Names
- Addresses
- Dates of birth
- Telephone numbers
- Emails
- Proof of identification (e.g. driver's license, passport information, utility bills)
- Emails
- IP addresses and other similar technical information required to provide the applicable services.

Frequency of the transfer (as applicable)

On a continuous basis as required by the Services Agreement.

Maximum data retention periods

Customer Personal Data will be retained for the duration of the services, subject to any requirement (i) to retain information in order to defend possible future legal claims; (ii) to comply with legal or regulatory requirements; (iii) to retain records; and/or (iv) to comply with any industry standards, guidelines and any contractual requirements agreed with Customer.

2 Definitions

Affiliate means any corporation, partnership, joint venture, or other entity that controls (whether directly or indirectly), is controlled by, or is under common control with a Party. For the purposes of this Addendum, Control means more than 50% of the aggregate stock or other interest entitled to vote on general decisions reserved to the stockholders, partners, or other owners of such entity.

Altus Group means the applicable legal entity that entered into the Services Agreement with Customer, including any Altus Group Affiliate.

CCPA means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and any implementing regulations thereof.

Customer means the entity which signs this Addendum as the Customer.

Customer Personal Data means personal data processed by Service Provider on behalf of the Customer for the purposes of supplying the Services pursuant to the Services Agreement and as further described in the Key Terms.

Data Protection Legislation means EU Data Protection Laws, UK Data Protection Laws, the CCPA and any other applicable data protection laws of any other country in relation to Customer Personal Data in respect of which the Service Provider is a Processor (or equivalent) under any other data protection laws.

Data Transfer Safeguard means a mechanism approved and/or permitted under Data Protection Legislation for data transfers ensuring that Customer Personal Data receives adequate protection, including adequacy decisions pursuant to Article 45 GDPR (and equivalent provisions of the Data Protection Legislation).

EU Data Protection Laws means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("**GDPR**") and laws implementing or supplementing the GDPR as amended, replaced or superseded from time to time.

Key Terms means clause 1 of this Addendum.

Restricted Transfer means a transfer of personal data (or an onward transfer), where such transfer would be prohibited by Data Protection Legislation (or by the terms of any data transfer agreements put in place to address the data transfer restrictions of Data Protection Legislation) in the absence of appropriate Data Transfer Safeguard(s), which may include: (a) a transfer of Customer Personal Data from the Customer to Service Provider; and/or (b) an onward transfer of Customer Personal Data from Service Provider to a Sub-processor.

Services means the products, software, technology, support, or other products and professional services Service Provider provides to Customer in accordance with the Services Agreement, including (as applicable) any subscription or licensed products, real estate consulting and advisory services, including property tax consulting services, agency services, lease consultancy services, valuation services, or other products and services the Service Provider makes available to Customer under the Services Agreement.

Standard Contractual Clauses means the standard contractual clauses for the transfer of personal data to third countries (implementing decision (EU) 2021/914 of 4 June 2021), or such clauses as may replace them from time to time.

Sub-processor means any person (including any third party, but excluding an employee) appointed by or on behalf of Service Provider to process Customer Personal Data in connection with the Services Agreement.

UK Addendum means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018.

UK Data Protection Laws means the Data Protection Act 2018, the "UK GDPR" as defined in section 3(10) of the Data Protection Act 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and other data protection or privacy legislation in force from time to time in the UK.

The terms **data controller**, **data processor**, **data subject**, **personal data**, **sell**, **share**, and **processing** shall have the meanings given in the Data Protection Legislation.

3 Agreed terms

- 3.1 The parties acknowledge that the Customer is the data controller and that Service Provider is a data processor of Customer Personal Data.
- 3.2 The Customer confirms that it has complied, and will continue to comply, with its obligations under the Data Protection Legislation in obtaining and processing Customer Personal Data, in particular that it has fairly and lawfully obtained the Customer Personal Data so as to enable Service Provider to provide the Services.
- 3.3 Service Provider is authorised to process Customer Personal Data to provide the Services and shall:
 - 3.3.1 process Customer Personal Data only in accordance with the Customer's instructions as are set out in this Addendum, as required to make available the Services or as provided in writing by the Customer from time to time (subject to Service Provider's right to charge additional sums at its current rates should the scope of the agreed Services be exceeded). Notwithstanding the foregoing, Service Provider may process Customer Personal Data as required under applicable law;
 - 3.3.2 notify the Customer immediately if it considers in its opinion that an instruction from the Customer is in breach of Data Protection Legislation, and Service Provider shall be entitled but not obliged to suspend execution of the instructions concerned, until the Customer confirms such instructions in writing;
 - 3.3.3 implement appropriate technical and organisational measures to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data. Should the Customer require Service Provider to apply or adapt security measures greater than those specified in the Services Agreement then Service Provider reserves the right to charge for doing so;

-
- 3.3.4 at the Customer's request and cost, taking into account the nature of the processing, assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, to assist with the Customer's obligation to respond to requests from data subjects of Customer Personal Data seeking to exercise their rights under Data Protection Legislation (to the extent that the Customer Personal Data is not accessible to the Customer through the Services);
- 3.3.5 at the Customer's request and cost, taking into account the nature of processing and the information available to Service Provider, assist the Customer with its obligations under Articles 32 to 36 of the GDPR (and equivalent provisions of the Data Protection Legislation);
- 3.3.6 ensure that personnel required to access the Customer Personal Data are subject to a binding obligation of confidentiality in respect of such personal data;
- 3.3.7 on reasonable request by the Customer not more than once annually, share any independent audit reports (e.g. ISO certifications and/or SOC reports) conducted in respect of the Altus Group with the Customer which Customer shall use to verify the Service Provider's compliance with Data Protection Legislation ("**Audit Reports**"). Customer shall treat such Audit Reports as Service Provider's confidential information. In the event that Customer is unable to satisfy its data protection audit rights afforded by Data Protection Legislation by reviewing such Audit Reports and such audit is required by a regulator, Service Provider will at the Customer's cost, allow the Customer, on prior written notice, to conduct a reasonable audit during business hours for the purpose of demonstrating compliance with Data Protection Legislation (provided that such audit right cannot be exercised more than once during the term of the Services Agreement unless otherwise required by a regulator). Such limited audit right shall be conducted in the least intrusive manner possible, and shall be subject to reasonable controls as may be determined by the Service provider to avoid risks to other clients/the security of the Altus Group environment and protect confidentiality; and
- 3.3.8 upon request by the Customer and at Customer's sole cost, use commercially reasonable efforts to delete or return to the Customer any such Customer Personal Data after the end of the provision of the Services, unless applicable law requires longer storage of the Customer Personal Data.
- 3.4 The Customer agrees that Service Provider may transfer Customer Personal Data or give access to Customer Personal Data to its Sub-processors for the purposes of providing the Services, provided that Service Provider complies with the provisions of this Clause 3.4. Service Provider shall remain responsible for its Sub-processor's compliance with the obligations of this Addendum. Customer pre-approves any Affiliate in Altus Group. A list of approved third party Sub-processors as of the date of this Addendum is available at [GDPR - Subprocessors | Altus Group](#), which shall be updated from time to time. Notwithstanding anything to the contrary in the Services Agreement, Customer expressly agrees that Service Provider can at any time and without justification appoint a new Sub-processor provided that the Customer is given thirty (30) days' prior notice and the Customer does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a Sub-processor's noncompliance with applicable Data Protection Legislation.
- 3.5 Insofar as the Service Provider's appointment of a Sub-processor involves a Restricted Transfer, the Service Provider shall ensure an appropriate Data Transfer Safeguard is in place with such Sub-processor(s)..
- 3.6 In respect of any Restricted Transfer to which GDPR applies, Service Provider and each Service Provider Affiliate (as "data importer") and Customer and each Customer Affiliate (as "data exporter") with effect from the commencement of the relevant transfer hereby enter into the Module 2 of the Standard Contractual Clauses in respect of any transfer from Customer (and/or Customer Affiliates) to a Service Provider (and/or Service Provider Affiliates) and:
- (a) Clause 7 – Docking clause of the Standard Contractual Clauses shall apply;
 - (b) Clause 9 – Use of Sub-processors of the Standard Contractual Clauses "Option 2" shall apply and the "time period" shall be 30 days;
 - (c) Clause 11(a) – Redress of the Standard Contractual Clauses, the optional language shall not apply;

-
- (d) Clause 13(a) – Supervision of Standard Contractual Clauses, the following shall be inserted where the data exporter is established in an EU Member State: “The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority” or, where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679 the following shall be inserted: “The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority (as appropriate)”
 - (e) Clause 17 – Governing law of the Standard Contractual Clauses “Option 1” shall apply and the “Member State” shall be Ireland
 - (f) Clause 18 – Choice of forum and jurisdiction of the Standard Contractual Clauses the Member State shall be Ireland;
 - (g) Annex 1 of the Standard Contractual Clauses shall be deemed to be pre-populated with the relevant sections of clause 1 “Key Terms” and the activities relevant to the transfer are delivery of the services under the Services Agreement; and
 - (h) Annex 2 of the Standard Contractual Clauses shall be deemed to be pre-populated with the relevant sections of Annex 1 to this DPA.

3.7 In respect of any Restricted Transfer to which the UK GDPR applies, Customer and Customer Affiliates (as “data exporter”) and Service Provider and Service Provider Affiliates (as “data importer”), hereby enter into the UK Addendum in respect of any transfer from Customer (and/or Customer Affiliates) to Service Provider (and/or Service Provider Affiliates) and agree that clause 3 above is amended by the provisions of Part 2 (Mandatory Clauses) of the UK Addendum and:

- (a) In respect of Table 1, the details are as found in this Addendum;
- (b) In respect of Table 2, the parties select Module 2 and the provisions of clause 3.6(a) to 3.6(c) of this Addendum shall apply;
- (c) Table 3 is populated per clause 3.6(g) and 3.6(h) of this Addendum shall apply to the UK Addendum; and
- (d) For the purposes of Table 4, the parties select “neither party”.

4 CCPA Terms

4.1 To the extent that Service Provider Processes any Customer Personal Data subject to the CCPA, Service Provider agrees to the following:

- 4.1.1 Service Provider is processing Personal Information subject to the CCPA for, or on behalf of, Customer, or Customer has made available Personal Information to Service Provider, for the business or commercial purpose(s) identified in the Agreement.
- 4.1.2 Service Provider shall not Sell, Share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Personal Information that Service Provider receives from, or on behalf of, Customer to any third party for monetary or other valuable consideration.
- 4.1.3 Service Provider shall not retain, use, or disclose Personal Information that Service Provider receives from, or on behalf of, Customer: (i) for any purpose (including, but not limited to, any commercial purpose) other than business purposes specified in the Agreement, or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Customer and Service Provider.
- 4.1.4 Service Provider may combine Personal Information that it receives from, or on behalf of, Customer with Personal Information that Service Provider receives from, or on behalf of, another person, or collects from its own interaction with an individual, unless the combining of

that Personal Information (1) would not be consistent with an individual's expectations, or (2) is prohibited by the CCPA. For avoidance of doubt, any restrictions on Service Provider's ability to combine Personal Information does not apply to Personal Information obtained by Service Provider prior to its engagement with Customer. For purposes of this Addendum, "combine" means to aggregate Personal Information about an individual into a single profile.

- 4.1.5 If Customer discloses deidentified Personal Information to Service Provider, or Service Provider deidentifies Personal Information previously disclosed by Customer, Service Provider shall take reasonable measures to ensure the deidentified Personal Information cannot be associated with a consumer or household and shall not attempt to reidentify the deidentified personal information.
- 4.1.6 Service Provider shall promptly notify Customer if Service Provider determines that it can no longer meet its obligations under this Addendum or the CCPA. Customer shall have the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information by Service Provider.
- 4.1.7 Service Provider certifies it understands the obligations and restrictions above and will comply with them.

5 Miscellaneous

- 5.1 The order of priority in the event of any conflict or inconsistency between the following documents shall be as follows: (1) any Data Transfer Safeguard, (2) this Addendum; and (3) the provisions of the Services Agreement. Save as specifically modified and amended in this Addendum, all of the terms, provisions and requirements contained in the Services Agreement shall remain in full force and effect and govern this Addendum.
- 5.2 Service Provider's obligations under this Addendum are given for the benefit of each Customer Affiliate. It is intended that a Customer Affiliate may enforce the benefits conferred on it under this Addendum in accordance with the terms of the *Contracts (Rights of Third Parties) Act 1999*, where applicable. A person who is not a party to this Addendum may not enforce any of its provisions, save to the extent set out in any applicable Data Transfer Safeguard. Notwithstanding this, any rights sought to be exercised, or remedies sought, pursuant to this Addendum by any Customer Affiliates shall solely be so exercised, or brought, by the Customer.
- 5.3 Limitation of Liability. The liability of each Party and its Affiliates, in aggregate, arising or related to this Addendum, shall in no event exceed the aggregate '*Limitation of Liability*' or other liability caps set forth in the Services Agreement, regardless of theory of liability, including but not limited to in contract, tort, warranty or any other theory. Service Provider and its Affiliates shall not be liable to any Customer Affiliate.
- 5.4 All capitalized terms not defined herein shall have the meaning set forth in the Services Agreement.
- 5.5 Service Provider reserves the right to charge Customer in respect of any further requests for cooperation or assistance which go beyond the commitments made in this Addendum.
- 5.6 The Parties' respective authorized signatories have duly executed this Addendum. Notwithstanding any other signatures contained in this Addendum belonging to an Affiliate, this Addendum is entered into by and between the Customer and the entity that Customer has contracted with in the Services Agreement.

Altus Group Limited

By: *Terrie-Lynne Devonish*
Printed Name: Terrie Devonish
Title: Chief Legal Officer
Date: Mar 15, 2023

Customer:

By:
Printed:
Title:
Date:

Altus Group (UK) Limited

By: *Terrie-Lynne Devonish*

Printed Name: Terrie Devonish

Title: Chief Legal Officer

Date: Mar 15, 2023

ARGUS Software (UK) Ltd.

By: *Terrie-Lynne Devonish*

Printed Name: **Terrie Devonish**

Title: Chief Legal Officer

Date: **Mar 15, 2023**

Finance Active SAS By:

Terrie-Lynne Devonish

Printed Name: Terrie Devonish

Title: Chief Legal Officer

Date: Mar 15, 2023

ANNEX 1: SECURITY MEASURES

1. Organization of information security

- (a) An information security management system based on industry acceptable best practices and standards.
- (b) An information security policy approved by senior management.
- (c) A management function dedicated to implementing and operating data protection and information security measures within the organization

2. Human resources security

- (a) Hiring and recruiting processes including screening of candidates and confidentiality and non-disclosure clauses in employment contracts for employees and contractors.
- (b) Information security awareness training for all employees.
- (c) A policy for acceptable use of electronic and internet communication systems and applications.

3. Asset security

- (a) A classification policy for information and data assets.
- (b) Asset handling procedures.

4. Access control

- (a) User registration and de-registration processes.
- (b) Control of privileged users.
- (c) Password and credentials policy.

5. Cryptography

- (a) Policy for implementing cryptographic controls, including email communication and Internet sites and services.

6. Physical security

- (a) Measures for the physical protection of data processing facilities and services.
- (b) Protection of unattended user equipment.

7. Operations security

- (a) Change management processes.
- (b) Measures for protecting against malicious software (malware) on computers, email services and Internet access.
- (c) Backup of data based on criticality and recovery requirements.
- (d) Logging and monitoring of security logs.

-
- (e) Installation of vendor issued security patches and hotfixes.

(f) Scanning for security vulnerabilities and weaknesses.

(g) Information security incident management.

8. Communications security

(a) Implementation of network boundary controls such as firewalls and intruder detection and prevention systems.

(b) Securing of wireless networks.

(c) Use of secure communication protocols for protecting network services.

9. System acquisition, development and maintenance (a)

Training developers in application development

security.

(b) Security testing of applications.

10. Supplier relationships

(a) Addressing confidentiality and non-disclosure in supplier agreements.