



## V1 DATA PROCESSING ADDENDUM

This Data Processing Addendum is entered into on the Effective Date; and is supplemental to all terms and conditions currently in place between the Customer and V1 but replaces any provisions in such terms and conditions relating to the processing of Personal Data by V1.

### IT IS HEREBY AGREED AS FOLLOWS:

1. The following definitions will apply:

**“V1”** means the contracting party set out in the Original Agreement, being a company, which is ultimately owned by the Holding Company;

**“Applicable Law”** means the laws of England and Wales (and any EU regulations from time-to-time retained or applicable under the terms of the European Union (Withdrawal Agreement) Act 2020 or applicable to services provided to EU customers);

**“Controller”** has the meaning set out in the Data Protection Legislation;

**“Customer”** means the contracting party set out in the signature block at the end of this Addendum;

**“DPA 2018”** means the Data Protection Act 2018 and any other applicable statutory provisions in the UK for the processing of information relating to individuals, the provision in connection with the UK’s Supervisory Authority functions under certain regulations, the provision for a direct marketing code of practice and for connected purposes.

**“Data Loss Event”** means any event that results, or may result, in unauthorised access to Personal Data held by V1 hereunder, and/or actual accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed in breach of Clause DP.

**“Data Protection Impact Assessment”** or **“DPIA”** means a process designed to help systematically analyse, identify and minimise the data protection risks of a project or plan, being a key part of accountability obligations under the Data Protection Legislation, and which helps to assess and demonstrate compliance with data protection obligations.

**“Data Protection Legislation”** means all applicable privacy or data protection laws and regulations (as amended, consolidated or re-enacted from time-to-time) which relate to the protection of individuals with regards to the processing of personal data to which a party is subject, including the DPA 2018 and UK GDPR for as long as any of the above are incorporated into Applicable Law together with any guidance and/or codes of practice issued from time-to-time by the relevant Supervisory Authorities;

**“Data Subject”** has the meaning set out in the Data Protection Legislation;

**“Data Subject Access Request”** means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;

**“EEA”** means the European Economic Area;

**“Effective Date”** means the date of signature hereof, or the 3 May 2023, whichever is sooner.

**“GDPR”** means 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;

**“Holding Company”** means Advanced Computer Software Group Limited (Co No 05965280) whose registered office is at The Mailbox Floor 3, 101 Wharfside Street, Birmingham, B1 1RF, UNITED KINGDOM;

**“ICO”** means Information Commissioner’s Office, the Supervisory Authority in the UK.

**“Original Agreement”** the terms and conditions currently in force between the parties;

**“Personal Data”** has the meaning set out in the Data Protection Legislation and includes (but is not limited to) special categories of personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, sex, sexual orientation, trade union membership or the processing of genetic or biometric data, for the purpose of uniquely identifying a natural person;

**“Personal Data Breach”** has the meaning set out in the Data Protection Legislation;

**“Processor”** has the meaning set out in the Data Protection Legislation;

**“Security Measures”** means appropriate technical and organisational measures which are set out in the service description (or other relevant documentation available) for the relevant products or services provided by the Processor;

**“Sub-processor”** means any third party appointed to process Personal Data on behalf of V1 related to the Original Agreement.

**“Supervisory Authority/ies”** means the relevant data protection regulatory authority located in the UK or EEA.

**“UK GDPR”** means UK General Data Protection Regulation retained from EU Regulation 2016/679.

2. In consideration of the ongoing provision of any services by V1 after the Effective Date of this Addendum the terms of this Addendum will be incorporated into the Original Agreement.
3. Notwithstanding any provisions in the Original Agreement relating to the protection of individuals with regards to the processing of Personal Data, such provisions will be superseded in their entirety and replaced by the following new Clause DP.
4. The following new Clause DP will be inserted into the Original Agreement, as follows:

- “DP.1 The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and V1 is the Processor.
- DP.2 V1 shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.
- DP.3 V1 shall provide reasonable assistance to the Customer in relation to compliance with the Data Protection Legislation.
- DP.4 V1 shall, in relation to any Personal Data processed in connection with its obligations to the Customer:
- DP.4.1 process that Personal Data only in accordance with the Schedule below, unless V1 is required to do otherwise by Applicable Law. If it is so required, V1 shall promptly notify the Customer before processing the Personal Data unless prohibited by Applicable Law;
  - DP.4.2 ensure that it has Security Measures in place (available on request) and the Customer hereby confirms that such Security Measures are appropriate to protect against a Data Loss Event having taken into account the:
    - DP.4.2.1 nature of the Personal Data to be protected;
    - DP.4.2.2 harm that might result from a Data Loss Event;
    - DP.4.2.3 state of technological development; and
    - DP.4.2.4 cost of implementing any additional measures;

In relation to DP.4.2, the parties acknowledge that the Processor may not be in a position to assess what measures are appropriate to the Controller's Personal Data (since the data is collected and processed for the purposes of the Controller's and not the Processor's business). The Controller may select chargeable services for additional security measures, based on the risk assessment of their data, which exceed the standard Security Measures provided by the Processor.

- DP.4.3 In relation to the clauses above, the Controller is responsible (as between the parties and to Data Subjects and supervisory authorities) for:
- DP.4.3.1 ensuring that they have a lawful basis for processing Personal Data, including appropriate consent, where applicable, to the processing of any Personal Data by the Processor;
  - DP.4.3.2 confirming the Security Measures meet the Data Protection Legislation standard of appropriateness;
  - DP.4.3.3 claims or complaints resulting from V1's actions to the extent that such actions directly result from instructions received from the Customer.
- DP.4.4 ensure that:
- DP.4.4.1 V1 personnel do not process Personal Data except in accordance with this Clause DP (and in particular the Schedule below);
  - DP.4.4.2 it takes all reasonable steps to ensure the reliability and integrity of any V1 or third party personnel who have access to the Personal Data and ensure that they: (i) are aware of and comply with V1's duties under this clause; (ii) are subject to appropriate confidentiality undertakings with V1 or any Sub-processor; (iii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Customer or as otherwise permitted hereunder; and (iv) have undergone adequate training in the use, care, protection and handling of Personal Data; and

DP.4.5 not transfer Personal Data outside of the EEA or outside of the UK unless the prior written consent of the Customer has been obtained or already agreed in the Original Agreement and the following conditions are fulfilled:

DP.4.5.1 the Customer or V1 has provided appropriate safeguards in relation to the transfer as determined by the Customer;

DP.4.5.2 the Data Subject has enforceable rights and effective legal remedies;

DP.4.5.3 V1 complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses all reasonable endeavours to assist the Customer in meeting its obligations); and

DP.4.5.4 V1 complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

**IT BEING ACCEPTED** by the Customer that:

DP.4.5.5 the geographical location of data hosting is in the UK, either in an V1 datacentre or a third party datacentre (or cloud managed service provider based in the UK), unless otherwise stated or agreed in the Original Agreement;

DP.4.5.6 the Customer is responsible for establishing the lawful basis of data transfer, including obtaining any necessary consent from Data Subjects to V1 in the UK;

DP.4.5.7 it is technically possible for hosted systems to be accessed by the Customer from outside the UK and EEA;

DP.4.5.8 the Customer is responsible for obtaining any necessary consent from Data Subjects in relation to any access by the Customer or licensed third parties to such hosted systems from outside the UK or EEA; and

DP.4.5.9 the Customer is liable for any complaints or claims by Data Subjects or third parties resulting from such access.

DP.4.6 at the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination unless V1 is required by Applicable Law to retain the Personal Data.

DP.5 Before allowing any Sub-processor to process any Personal Data related hereto V1 must give the Customer:

DP.5.1 at least 30 calendar days' notice in writing of the intended Sub-processor and processing;

DP.5.2 confirmation that there is a written agreement with the Sub-processor which give effect to the terms set out in this Clause DP such that they apply to the Sub-processor;

DP.5.3 such information regarding the Sub-processor as the Customer may subsequently reasonably require.

V1 shall remain fully liable for all acts or omissions of any Sub-processor.

DP.6 V1 currently provides software development and support services from outside the UK and EEA through Advanced Business & Healthcare Solutions India Private Ltd, the wholly owned subsidiary, of its Holding Company, which conforms to all necessary requirements and appropriate safeguards under Applicable Law. No physical transfer of Data takes place during the provision of such development or support services. Controlled remote access is granted to the staff in India only for the limited purposes of software development and support services. Personal Data will be anonymised wherever reasonably practicable to do so in the timeframes available. Compliance with Applicable Law can be provided in writing to the Customer in this regard.

DP.7 Subject to Clause DP.4, V1 shall notify the Customer immediately but no later than 72 hours of receipt if it:

DP.7.1 receives a Data Subject Access Request (or purported Data Subject Access Request) relevant to the Customer;

DP.7.2 receives a request to rectify, block or erase any Personal Data relevant to the Customer;

DP.7.3 receives any other request, complaint or communication relating to either party's obligations under the Data Protection Legislation;


DP.7.4 receives any communication from a Supervisory Authority or any other regulatory authority in connection with Personal Data, relevant to the Customer, processed hereunder;

- DP.7.5 receives a request from any third party relevant to the Customer for disclosure of Personal Data where compliance with such request is required or purported to be required by Applicable Law; or
- DP.7.6 becomes aware of a Data Loss Event relevant to the Customer or a Personal Data Breach relevant to Data Subjects of the Customer.
- DP.8 V1's obligation to notify a Personal Data Breach under Clause DP.7 shall include the provision of further information to the Customer in phases as details become available.
- DP.9 Taking into account the nature of the processing, V1 shall provide the Customer with full assistance in relation to either party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause DP.7 (within the timescales agreed between the parties) including by promptly providing:
- DP.9.1 the Customer with full details and copies of the complaint, communication or request;
- DP.9.2 such assistance as is reasonably requested by the Customer to enable the Customer to comply with any request related to the Data Subject's rights within the relevant timescales set out in the Data Protection Legislation;
- DP.9.3 the Customer, at its request, with any Personal Data it holds in relation to a Data Subject;
- DP.9.4 assistance as requested by the Customer following any Data Loss Event;
- DP.9.5 assistance as requested by the Customer with a Data Protection Impact Assessment (at the Customer's cost where there is any significant level of work required);
- DP.9.6 assistance as requested by the Customer with respect to any request from the Information Commissioner's Office, or any consultation by the Customer with the Supervisory Authority.
- DP.10 V1 shall maintain complete and accurate records and information to demonstrate its compliance with the Data Protection Legislation.
- DP.11 V1 shall allow customers to request evidence of compliance with Data Protection Legislation as part of the Customers' supplier audit processes, at reasonable times, and at reasonable notice. The Processor will be responsible for reasonable costs in this regard but may levy a charge for costs incurred which it considers unreasonable, in complying with an audit. Where a non-conformity is detected and the cause is solely a material breach of V1's data processing obligations under Applicable Law and/or V1's failure to provide the Security Measures that it is contractually committed to provide, any costs related to the remediation of these non-conformities shall be borne by V1.
- DP.12 For the avoidance of doubt, notwithstanding anything to the contrary in the Original Agreement, each party accepts liability for loss of Personal Data to the extent that the loss of Personal Data is caused by:
- a material breach by such party of their data processing obligations under Applicable Law;
  - a failure by such party to provide the Security Measures that it was contractually committed to provide in relation to such Personal Data

UP TO THE SUM OF 100% OF THE TOTAL CHARGES AND RESULTING SUMS PAID (EXCLUDING VAT AND EXPENSES) BY THE CUSTOMER TO V1 IN THAT YEAR; FOR THE PURPOSES OF THIS CLAUSE, "YEAR" SHALL MEAN A PERIOD OF 12 MONTHS (OR SHORTER PERIOD IN THE PERIOD IMMEDIATELY PRIOR TO TERMINATION OF THE AGREEMENT) COMMENCING ON THE EFFECTIVE DATE OF THIS MASTER AGREEMENT OR ANY ANNIVERSARY OF SUCH EFFECTIVE DATE."

5. Notwithstanding anything to the contrary set out in the Original Agreement, to the extent that there is any duplication or conflict between definitions or clauses used in the Original Agreement and this Addendum, the definitions and clauses set out in this Addendum will apply and take precedence. In all other respects the Original Agreement as amended by this Addendum shall continue in full force and effect.
6. Each party confirms that their signatory set out below is a duly authorised representative and authorised to act on behalf of the relevant party. All the terms of Clause DP are expressly confirmed and consented to by the Customer hereunder.
7. This Addendum is governed by the laws of England and Wales and the parties submit to the exclusive jurisdiction of the courts of England and Wales.

In witness of which the parties have agreed to this Addendum and executed this Addendum by their duly authorised representatives

For and on behalf of <b>V1</b>		For and on behalf of the <b>Customer</b>	
Authorised Signatory		Customer Company Name	
		Authorised Signatory	
Name	Stephen Dews	Name	
Position	Group CFO	Position	
Date	3 May 2023	Date	

**Schedule**

1. V1 shall comply with any further written instructions of the Customer with respect to processing by V1. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	<p>The services purchased by the Controller, as detailed in the Order Form,</p> <ol style="list-style-type: none"> <li>1. Hosting – Cloud and platform</li> <li>2. Software Support services</li> <li>3. Bespoke software development</li> <li>4. Project Management</li> <li>5. Training &amp; Consultancy</li> <li>6. Payroll services</li> <li>7. IT services</li> <li>8. Managed Services / IT Outsourcing Services</li> <li>9. Migration services</li> <li>10. Other professional services</li> <li>11. Research and analytics purposes</li> </ol>
Duration of the processing	The term of the Original Agreement
Nature and purposes of the processing	<p>Nature of Processing:</p> <ol style="list-style-type: none"> <li>1. Storage</li> <li>2. Access</li> <li>3. Consultation</li> <li>4. Remote Access</li> <li>5. Deletion</li> <li>6. Alteration</li> <li>7. Anonymisation of data</li> </ol> <p>Purposes of processing: Any of the following services stated in the Order Form.</p> <ol style="list-style-type: none"> <li>1. Hosting – Cloud and platform</li> <li>2. Software Support services</li> <li>3. Bespoke software development</li> <li>4. Project Management</li> <li>5. Training &amp; Consultancy</li> <li>6. Payroll services</li> <li>7. IT services</li> <li>8. Managed Services / IT Outsourcing Services</li> <li>9. Migration services</li> <li>10. Research and analytics purposes</li> <li>11. Other professional services</li> </ol>
Type of Personal Data	Personal Data and/or Special Category data relating to individuals provided to V1 by, or at the direction of, the Customer in connection with the Services.
Categories of Data Subject	This varies from customer to customer. The Customer will maintain a list of categories of data subjects appropriate to their use of the software or services.

Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data

On termination or expiry of the Original Agreement, V1 will return the Customer's personal data in a standard machine-readable format (at the Customer cost or as otherwise agreed in writing between the parties) upon receipt of a documented request from the Customer. Such request must be sent within thirty (30) days of expiry or termination of the Original Agreement. Once the Original Agreement has expired or terminated, any Personal Data will be immediately put beyond use and, after ninety (90) days of expiry or termination of the Original Agreement, it will be deleted. In the event that the Customer does request return of their Personal Data as described above, all Personal Data will be deleted within ninety (90) days of the confirmation of receipt of data extract by the Customer, unless otherwise agreed in writing between the parties or to the extent it is required to be retained or deleted under Data Protection Legislation.