Charterhouse Group Data Processing Agreement

1. Application, Definitions, and Interpretation

1.1. This data processing agreement (**"DPA"**) forms part of the Supplier General Terms and Conditions ("**Agreement**") and is made effective from the date of the Agreement. Save as otherwise set out in this DPA, the Agreement shall remain in full force and effect.

1.2. Capitalised terms used but not defined in this DPA shall have the meanings as set out in the Agreement, and capitalised terms used as defined below shall have the meaning set out in this DPA. To the extent of any conflict between a defined term in this DPA and in the Agreement, for the purposes of this DPA only, the defined terms set out in this DPA shall prevail.

1.3. Definitions:

(a) **"Customer Personal Data"** means any Personal Data provided to Supplier for Processing as part of the provision of the Services;

(b) **"Data Processing Instructions"** means the Processing activities which may be performed by Supplier in relation to Customer Personal Data, as set out in the Schedule;

(c) **"Data Protection Legislation"** means all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (DPA 2018); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications), and with the terms "Data Controller", "Data Processor", "Data Subject", "Personal Data", "Personal Data Breach", and "Processing" shall have the meanings set out in Data Protection Legislation;

(d) **"Services"** means the services set out in an Order Form;

(e) **"Standard Contractual Clauses"** means model clauses approved by the Supervisory Authority, including the UK ICO's International Data Transfer Agreement, or International Data Transfer Addendum (as appropriate), which enable the export of Personal Data to a territory has not been deemed adequate for data protection purposes under Data Protection Legislation;

(f) **"Subprocessor"** means any person or entity appointed by or on behalf of the Processor to process personal data on behalf of the Controller;

(g) **"Supervisory Authority"** means, in the case of the United Kingdom, the Information Commissioner;

(h) **"Territory"** means the United Kingdom and European Economic Area; and

1.4. **"Data Controller"**, **"Data Processor"**, **"Data Subject"**, **"Personal Data"**, **"Personal Data Breach"**, and **"Processing"** shall have the meanings set out in Data Protection Legislation.

1.5. The rules of interpretation set out in the Agreement shall apply to this DPA.

2. Relationship between the Parties

2.1. Where Supplier provides any Services to the Customer which involves any of the activities set out in the Data Processing Instructions, the Customer, as Data Controller, instructs Supplier, as Data Processor, to Process the Customer Personal Data in accordance with this DPA.

3. Data Processing

3.1. Each Party shall comply with Data Protection Legislation as it relates to the Agreement.

3.2. The Customer is solely responsible for establishing the lawful basis for the processing of Customer Personal Data by Supplier under the Agreement, including where applicable the obtaining of all necessary consents from Data Subjects, and shall notify Supplier on request of the applicable lawful basis for any processing Supplier is required to perform.

3.3. In respect of the Processing of Customer Personal Data, Supplier shall:

(a) only act on the documented written instructions of the Customer;

(b) immediately inform the Customer if, in its opinion, an instruction infringes Data Protection Legislation; and

(c) only process Customer Personal Data other than in accordance with clause 3.3(a) only if required to do so by law, in which case Supplier shall inform the Customer of the relevant legal requirement before processing (unless that legal requirement prohibits such information being provided to the Customer on the grounds of public interest).

3.4. The Data Processing Instructions sets out the subject matter and other details regarding the Processing of the Customer Personal Data contemplated as part of the Services, including Data Subjects, categories of Personal Data, special categories of Personal Data, Subprocessors and description of Processing. Supplier may update the Data Processing Instructions from time to time to reflect changes to the solutions which may form part of the Services.

4. Supplier Personnel

4.1. Supplier shall ensure that persons authorised to undertake Processing of Customer Personal Data have:

(a) committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and

(b) undertaken appropriate training in relation data protection;

5. Security

5.1. 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, Supplier shall in relation to the Customer Personal Data implement appropriate technical and organisational measures designed to provide a level of security appropriate to that risk in the provision of the Services. The Supplier details its security measures through its Information Security Schedule, available upon request.

6. Subprocessing

6.1. Customer acknowledges that the Services may involve the appointment of Subprocessors, as further outlined in the Data Processing Instructions. Customer authorises the appointment of such Subprocessors in accordance with this DPA, including data centre operators, cloud service providers and support providers, in each case where applicable to support the delivery of the Services.

6.2. Where Subprocessors are engaged, Supplier shall:

(a) inform the controller of any intended changes concerning the addition or replacement of Subprocessors;

(b) implement a written contract containing substantially similar data protection obligations as set out in this agreement, 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 Data Protection Legislation; and

(c) remain liable to the Customer for the performance of the Subprocessor's obligations.

6.3. Supplier may inform the Customer of any such change to Subprocessors by either (i) notifying the Customer by email, or (ii) updating the list of Subprocessors in the Data Processing Instructions and publishing such updated list to the Supplier website. Where the Customer has an objection to the appointment of any new Subprocessor, provided such objection relates to Data Protection Legislation, Customer must notify Supplier promptly and in any event within fourteen (14) days of such notice. Both Parties shall discuss in good faith measures to address any such objection.

Charterhouse Group Data Processing Agreement

6.4. Customer acknowledges and accepts that Subprocessors themselves may appoint their own subprocessors, Subprocessors will either publish a list of their own subprocessors on their website or provide or provide this information upon request.

7. Assisting the Customer

7.1. Supplier shall, having regard to the nature of the Services, the Processing, and the information available to Supplier, provide reasonable assistance to the Customer upon written request:

(a) in meeting the Customer's obligations under the Data Protection Legislation with respect to data security, breach notification, data protection impact assessments and prior consultation with or notification to a competent data protection supervisory authority;

(b) by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights, as provided for in Data Protection Legislation; and

(c) makes available to the Customer all information necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, provided that to meet this request, Supplier may provide confidential extracts of audit reports, certificates demonstrating compliance with relevant standards, and other information which Supplier may reasonably determine, and Customer acknowledges and accepts that on-site visits are not possible.

7.2. Where any assistance requested pursuant to this clause 7 involves more than one (1) day of effort, Supplier reserves the right to charge Customer for the applicable Professional Services at its then current rates.

8. Personal Data Breach

8.1. Supplier shall notify the Customer without undue delay upon becoming aware of a Personal Data Breach, providing the Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under Data Protection Legislation. Such notification shall at a minimum:

(a) describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

(b) communicate the name and contact details of Supplier's data protection officer or other relevant contact from whom more information may be obtained;

(c) describe the likely consequences of the Personal Data Breach in so far as Supplier is able to ascertain having regard to the nature of the Services and the Personal Data Breach; and

(d) describe the measures taken or proposed to be taken to address the Personal Data Breach.

8.2. Supplier shall co-operate with Customer and take such reasonable steps as are necessary to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

8.3. Where and in so far as, it is not possible to provide the information referred to in this clause 8.1 at the same time, the information may be provided in phases without further undue delay.

9. Deletion or Return of Customer Personal Data

9.1. Within thirty (30) days from termination or expiry of the Agreement (the "Return Period"), and subject to Section 9.4 below, at Customer's request, Supplier will either delete or return available Customer Personal Data. At the expiry of the Return Period, if the Customer has not elected either of the foregoing Supplier may delete and destroy all Customer Personal Data without notice or liability to Customer.

9.2. Where Customer requests Supplier return available Customer Personal Data, Supplier may fulfil this request by making Customer aware of functionality within the Services that enables Customer to retrieve the Customer Personal Data without additional Processing by Supplier. If Customer declines to use this functionality, Customer may, within the Return Period, request that Supplier return the available Customer Personal Data under an Order for the applicable Professional Services.

9.3. Supplier shall provide written confirmation to Customer that it has fully complied with this Section 9 within thirty (30) days of Customer's request for such confirmation.

9.4. Supplier may retain Customer Personal Data to the extent required by Data Protection Legislation and only to the extent and for such period as required by Data Protection.

10. International Data Transfers

10.1. Supplier is established and primarily operates in the United Kingdom, and Supplier's primary data storage and cloud hosting locations are in the Territory.

10.2. Further to clauses 6.1 and 6.4, Customer acknowledges and accepts that provision of the Services may involve the export of Customer Personal Data outside the Territory. Subprocessors will either publish a list of such jurisdictions on their website or provide this information upon request.

10.3. Supplier will only export Customer Personal Data outside of the Territory:

(a) where the recipient is in a jurisdiction deemed to have an adequate level of data protection;

(b) where the recipient has binding corporate rules;

(c) where the recipient is subject to Standard Contractual Clauses; or

(d) where the recipient is subject to a code of conduct or approved certification mechanism,

in each case, in a form, or otherwise, as approved by the Supervisory Authority.

10.4. Supplier may conclude Standard Contractual Clauses in the name of Supplier but for the benefit of Customer as it relates to the provision of the Services, and Customer authorises Supplier to conclude such agreement in Supplier's own name, and acknowledges and accepts that such agreement may be for the benefit of multiple customers.

11. Notices

11.1. The Supplier Data Protection Officer can be contacted by email at privacy@cvdgroup.com. The Customer may provide, by email to the foregoing address, details of the Customer's primary point of contact for the purposes of any notices arising from this DPA.

Charterhouse Group Data Processing Agreement

Schedule – Data Processing Instructions

Data Processing Overview	These Data Processing Instructions form part of the Terms & Conditions, and should be read in conjunction with the clauses relating to Data Processing and Security. This table sets out the circumstances in which Supplier may be considered a Data Processor for the Customer, and the related categories of data, data subjects and vendors. Due to the breadth of the Supplier offering, the nature of data processing for each customer will vary depending on the solutions deployed. In this table Supplier sets out the most common processing types Supplier perform for our customers. Supplier work closely with our vendors, and in some cases those vendors may be considered sub-processors for Supplier or direct processors for the Customer. Customers may receive Services which comprises multiple solutions. The Order Form(s) will set out the solutions procured by the Customer.	
Supplier Processing Activity	**Professional Services**	Where a Customer engages Supplier to provide Professional Services, including configuration, installation, consulting, or other Services, then Supplier may process Customer Personal Data as part of this engagement. Professional Services are primarily delivered at the outset of a project but may also be performed during the term. This processing may relate to either on-premise or hosted solutions and may involve the sharing of Customer Personal Data with third party vendors who deliver elements of the Services. The Customer Personal Data processed as part of a Professional Services engagement will vary depending on the nature of the solution(s) to which the engagement relates, and additional information on the project is typically set out in a statement of work or high level design document.
	Support Services	Supplier provides customers with support and maintenance services through our support team in accordance with the Services Guide. The Service Desk is the Customer's point of contact to raise any incidents or service requests, and can be contacted by telephone, email or through the customer portal. The processing which may occur through the provision of Support relates to day-to-day Customer support requests in relation to the Services, including faults, errors, system failure, configuration queries, updates, and other issues. Login and contact information captured through the Support Services is dealt with in accordance with our Privacy Policy, as Supplier is a data controller of that Personal Data. Beyond the login and contact information, the Customer may provide Customer Personal Data as part of the Support request, including attachments, explanatory text, or other information which will be used to triage the request, and this Customer Personal Data will be processed by Supplier in accordance with the Agreement. Depending on the nature of the request, Supplier may need to remotely access the Customer's on-premise or hosted environment and as a result may have access to Customer Personal Data. In some cases, Supplier may need to escalate the Support case to a third party vendor which delivers elements of the Services. Additional information on the nature of the Service Desk is set out in the Service Guide.
	Cloud or Hosting Services	Cloud or Hosting Services may include (i) a subscription to an application of software as a service, or (ii) provision of infrastructure as a service, in each case managed either by Supplier or a third party vendor. Where the Customer subscribes to Cloud or Hosting Services, Customer through their use of the Cloud Services will upload, either manually or automatically, data to the Cloud Services to use the solution for business purposes. Some of the data which may be uploaded to the Cloud Services may include Customer Personal Data. Depending on the exact Cloud or Hosting Services procured, the specifics of the categories of data and data subjects will vary. Where Supplier are providing Managed Services or Support in relation to the Cloud Services, then Supplier will be Customer's Data Processor, and Supplier will appoint a third party hosting vendor to provide the infrastructure elements of the Services. Where Supplier is only reselling Cloud or Hosting Services, and not providing any value-added services like managing the environment or providing support, Supplier will not be considered a Data Processor. In those circumstances the vendor delivering the Services will be the Customer's Data Processor and their data processing agreement will apply.
	Managed Services	Managed Services may involve a combination of Professional Services, Support and/or Cloud or Hosting Services, delivered as an overall service. This may also include several different products or solutions, each of which may involve different third party vendors. As part of delivering the Managed Services, Supplier may process Customer Personal Data either provided to Supplier by the Customer or collected by Supplier for and on behalf of the Customer. Supplier provide multiple Managed Services, including managing the Customer's: local area network, wide area network, telephony and unified communications, and cyber-security. Usually only a very small amount of data processed will involve Customer Personal Data, if any.
Supplier as a **Data Controller**	As part of our day-to-day interaction with the Customer, Supplier may be considered a Data Controller in the circumstances set out in our Privacy Policy. These include marketing, finance, billing, processing orders, and account management. For the avoidance of doubt, Supplier does not become a Data Controller of Customer Personal Data. Supplier will process Personal Data for which it is a Data Controller in accordance with the Privacy Policy and this is outside the scope of the Agreement.	
Categories of Personal Data	The Categories of Personal Data will vary depending on the solution(s) and configuration, but common categories of Personal Data are: • Customer's employees: name, title, email, telephone number, department, ID number, contact history, system usage, call durations, job title, IP address, and login credentials. • Customer's end-customers: name, title, email address, telephone number, contact history, account number, and IP address. Additional categories of Personal Data may be provided by Customer or collected by Supplier on behalf of the Customer either as part of (i) the Professional Services engagement, (ii) a Support request, (iii) through Cloud or Hosting Services, or (iv) through the Managed Services.	
Special Category Data	As additional categories of Personal Data may be provided by Customer as noted above, it is possible that from time-to-time Customer instructs Supplier to Process special categories of Personal Data. Due to the solutions and services Supplier provides, some solutions are less likely than others to involve any special categories of Personal Data. Where applicable, Customer must inform Supplier of this intention prior to instructing this Processing.	
Data Subjects	The data subjects will vary depending on the solution(s) and configuration, but common data subjects are: • Employees, clients, end-customers and suppliers of Customer • Employees or contractors of Customer who contact Supplier's Service Desk The Customer determines which Data Subjects form part of the Processing and therefore these categories may change depending on Customer's use of the solution(s).	
Duration of Processing	The duration of processing will vary depending on the solution(s) and configuration, but common durations are: • Support and Professional Services: Personal Data is processed only for as long as is necessary to provide the Support and/or Professional Services. • Cloud or Hosting Services and Managed Services: Personal Data is stored for the duration of the Services and is deleted or returned to Customer as set out in the data processing agreement or as otherwise amended or deleted by Customer during the Term.	
Third Party Vendors (Subprocessors)	As noted throughout these Data Processing Instructions, depending on the solution(s) and configuration, third party vendors may be engaged either as a sub-processor to Supplier, or as a direct processor to the Customer. The Order Form(s) will set out the solutions procured by the Customer, and these Order Forms, together with any statement of work, high level design, end user agreement, or other supporting documentation, may also identify such vendor(s). Third party vendors may be engaged in any of the above processing activities, for the following purposes: • Professional Services: to assist in the implementation or configuration of the solution(s), whether as the software or equipment vendor, or a third party subcontractor to Supplier. • Support Services: in the case of the solution vendor or equipment manufacturer, to provide support in cases requiring escalation from the Supplier Service Desk, or a third party subcontractor to Supplier to provide overflow or out of hours support. • Cloud or Hosting Services: to provide the supporting infrastructure, software as a service, or other services cloud or hosting services. • Managed Services: to provide the supporting infrastructure, software as a service, monitoring, alert detection, direct routing, or other services which forms part of the Managed Services. Supplier's most common third party vendors are listed on this page. By proceeding to place the Order, you confirm that you authorise the appointment of these vendors as subprocessors, or processors (as applicable) for the Services. Additional information on each of the vendors and their data processing credentials is available from Supplier upon request.	