# Data Processing Agreement

Version 1.1.
April 2024.

# Table of Contents

This Data Processing Addendum (“DPA”) is incorporated into our Service Agreement and all related orders between Customer and virtualDCS and reflects the parties’ agreement about the processing of Data (as these terms are defined below). This DPA consists of the main body of the DPA and Appendix 1.

## 1. Definitions

"**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in EU/UK Data Protection Law.

“**Affiliate**” means an entity which is controlling, controlled by or under common control with a party. For purposes of this definition, "control" means possessing, directly or indirectly, the power to direct or cause the direction of the management, policies or operations of an entity, whether through ownership of voting securities, by contract or otherwise.

"**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations applicable to the personal data in question, including, where applicable, EU/UK Data Protection Law.

"**Customer**" means the party which entered into the Service Contract, or an Affiliate thereof, and signatory to this DPA.

"**Data**" has the meaning given to it in Appendix 1.

"**DPA**" means this Data Processing Addendum.

"**EU/UK Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time.

“**Service Agreement**” means each applicable order for the Services the Customer has purchased from virtualDCS.

"**virtualDCS**" means Virtual Data Centre Service Limited. or the Affiliate thereof who has entered into the Service Agreement with the Customer.

"**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject to an adequacy determination based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"**Security Incident**" has the meaning given to it in Clause 2.8.

“**Self-Service Tools**” means functionality which may be me available by virtualDCS in the software licensed or made available to Customer which permits Customer to comply with controller obligations under Applicable Data Protection Law relevant to Customer’s use of the Services.

"**Services**" means the services provided by virtualDCS to Customer under or in connection with the Service Agreement.

"**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

“**TOMs**” means the security provisions as set out in appendix 2.

## 2. Processing Data

2.1 **Relationship of the parties**: Customer (the controller) appoints virtualDCS as a processor to process the personal data that is the subject of the Service Agreement and as further described in Appendix 1 (the "**Data**").

2.2 **Prohibited data**: Customer shall not disclose (and shall not permit any data subject to disclose) any sensitive data (special categories) of Data or Data that imposes specific data security or data protection obligations on  in addition to or different from those specified in this DPA or the Service Agreement to virtualDCS for processing except where and to the extent expressly disclosed in Appendix 1.

2.3 **Term and termination**: The term of this DPA, including its Appendices, shall continue until all processing of Customer's personal data by virtualDCS ceases.

2.4 **Purpose limitation**: virtualDCS shall process the Data as a processor as necessary to perform its obligations under the Service Agreement, including for the purposes described in Appendix 1 to this DPA and strictly in accordance with the documented instructions of Customer (the "**Permitted Purpose**"), except where otherwise required by law(s) that are not incompatible with Applicable Data Protection Law. In no event shall virtualDCS process the Data for its own purposes or those of any third party.

Each party is solely responsible for compliance with its respective obligations under Applicable Data Protection Law. The Customer shall comply with all necessary transparency and lawful requirements under Applicable Data Protection Law in order to disclose the Data to virtualDCS for the Permitted Purposes. virtualDCS shall immediately inform Customer if it becomes aware that Customer's processing instructions infringe Applicable Data Protection Law (but without obligation to actively monitor Customer's compliance with Applicable Data Protection Law).

If a change in Applicable Data Protection Law prevents virtualDCS from processing the Data as intended by the Service Agreement, Customer will immediately stop transmission of the Data to virtualDCS and the parties will negotiate in good faith changes to the Service Agreement which may include but are not limited to additional services or solutions, if and when made available by virtualDCS. Notwithstanding anything to the contrary, data localization laws in Applicable Data Protection Law shall not require virtualDCS to change the storage location of any data centres agreed in, or permitted by, the Service Agreement;

provided that virtualDCS will negotiate in good faith commercially-reasonable changes to the storage location.

2.5 **Restricted transfers**: The parties agree that when the transfer of Data from Customer to virtualDCS is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

a. in relation to data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:
   i. Module Two will apply;
   ii. in Clause 7, the optional docking clause will apply;
   iii. in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 10 of this DPA;
   iv. in Clause 11, the optional language will not apply;
   v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
   vi. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
   vii. Annex I of the EU SCCs shall be deemed completed with the information set out in Appendix 1 to this DPA; and
   viii. Annex II of the EU SCCs shall be deemed completed with the TOMs.

b. in relation to data that is protected by the UK GDPR, the UK SCCs will apply and the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**") shall be deemed executed between Customer and virtualDCS and completed as follows:
   i. The EU SCCs, completed as set out above in clause 2.5(a), shall apply to transfers of such Data, and the EU SCCs shall be deemed amended as specified by Part 2 of the UK Addendum in respect of the transfer of such Data.
   ii. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out above at clause 2.5(a) (as applicable), the TOMs and in Appendix 1 of this DPA, and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

c. in the event that any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

2.6 **Onward transfers**: virtualDCS shall not participate in (nor permit any subprocessor to participate in) any other Restricted Transfers of Data (whether as an exporter or an importer of the Data) unless the Restricted Transfer is made in full compliance with Applicable Data Protection Law.

2.7 **Confidentiality of processing**: virtualDCS shall ensure that any person that it authorises to process the Data (including virtualDCS's staff, agents and subprocessors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Data who is not under such a duty of confidentiality. virtualDCS shall ensure that all Authorised Persons process the Data only as necessary for the Permitted Purpose.

2.8 **Security**: virtualDCS shall implement and maintain appropriate technical and organisational measures as set out in the TOMs to protect the Data from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access (a "**Security Incident**").

2.9 **Updates to security measures**: The technical and organizational measures are subject to technological progress and advancements. As such, virtualDCS may implement alternative, adequate measures which meet or exceed the security level of the measures described in the TOMs.

2.10 **Subprocessing**: Customer consents to virtualDCS engaging virtualDCS Affiliates and third party subprocessors to process the Data for the Permitted Purpose provided that: (i) virtualDCS maintains an up-to-date list of its subprocessors that may process personal data. These lists are available upon request via Customer’s normal contacts for the applicable Services or may be published in the documentation portal for the applicable Service, and virtualDCS shall update such lists with details of any change in subprocessors at least 10 days' prior to any such change; (ii) virtualDCS imposes data protection terms on any subprocessor it appoints that protect the Data, in substance, to the same standard provided for by this DPA; and (iii) virtualDCS remains liable for any breach of this DPA that is caused by an act, error or omission of its subprocessor.

2.11 **Cooperation and data subjects' rights**: Taking into account the nature of the processing and to the extent a response to a request cannot be achieved using the Service's Self-Service Tools available to the Customer, virtualDCS will provide commercially reasonable assistance to the Customer (at Customer's expense) to: (i) fulfil a Customer's obligation to respond to data subjects' requests under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) in relation to any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. If any such request, correspondence, enquiry or complaint is made directly to virtualDCS, virtualDCS shall promptly inform Customer providing full details of the same.

2.12 **Data Protection Impact Assessment**: virtualDCS shall, which may be subject to reimbursement of virtualDCS's then-current hourly fees, provide Customer with all such reasonable and timely assistance as Customer may require in order to conduct a data protection impact assessment in accordance with Applicable Data Protection Law.

2.13 **Deletion or return of Data**: Upon termination or expiry of the Service Agreement, virtualDCS shall destroy all Data (including all copies of the Data) in its possession or control, except as otherwise stated in the Service Agreement. This requirement shall not apply to the extent that virtualDCS is required by any applicable law to retain some or all of the Data, or to Data it has archived on back-up systems, in which event virtualDCS shall isolate and protect the Data from any further processing except to the extent required by such law until deletion is possible.

2.14 **Data records**: Documentation materials that serve as evidence that Data was processed in a proper manner consistent with the stipulations of this DPA may be stored by virtualDCS after termination of this DPA in accordance with the applicable retention periods.

2.15 **Audit**

a. Customer may audit virtualDCS’s compliance of its obligations under this DPA, at its own expenses by itself or by a certified auditor. Customer shall provide at least 60 days, prior written notice of its intention of doing so and virtualDCS shall make available all information reasonably necessary to demonstrate such compliance, and shall allow for and contribute to audits, including inspections, by Customer. Such audits shall be conducted during regular business hours and Customer shall ensure that it does not disrupt the regular operations of virtualDCS. Customer will not exercise its audit rights more than once in any twelve (12) month period (in aggregate with any information rights in the Service Agreement), except (i) if and when required by instruction of a competent data protection authority; (or) if Customer believes a further audit is necessary due to a Security Incident suffered by virtualDCS. For any audit or right of access exercised under this section, the SCCs or any similar right granted by law, virtualDCS will not be required to: (x) provide information, evidence or access of any kind that includes other customers' information, and to preserve the rights, confidentiality, security, and data integrity of other customers; or (y) provide any access to or inspections of any of its premises, networks, systems, equipment or other infrastructure of virtualDCS or its subprocessors.

b. Alternatively at virtualDCS's discretion and if available for the applicable Service, virtualDCS may satisfy its obligations under this Clause (*Audit*) (and any similar obligations under the Standard Contractual Clauses) by presenting a summary copy of its ISO 27001 audit or certification report(s) to Customer, which reports shall be subject to the confidentiality provisions of the Service Agreement.
c. Customer shall be responsible for all costs and fees, including all reasonable costs and fees for any and all time virtualDCS expends for any such audit.
d. All information disclosed or developed as a result of an audit and inspection constitutes Confidential Information of virtualDCS.

2.16 **Governing law:** This DPA shall be governed by the laws of same jurisdiction as agreed in the Service Agreement.

# Appendix 1

This Appendix 1 forms part of the DPA and describes the processing that the processor will perform on behalf of the controller.

## A. List of parties

**Controller(s) / Data exporter(s)**: [*Identity and contact details of the controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

| | |
|---|---|
| **Name:** | Customer (as defined in the applicable Service Agreement) |
| **Address:** | As defined in the applicable Service Agreement or as otherwise provided by the Customer |
| **Contact person's name, position, and contact details:** | Customer's point of contact for notices or as otherwise provided by Customer |
| **Activities relevant to the data transferred under this DPA:** | The Services |
| **Role (controller/processor):** | Controller |

**Processor(s) / Data importer(s)**: *[Identity and contact details of the processor(s) /data importer(s), including any contact person with responsibility for data protection*]

| | |
|---|---|
| **Name:** | virtualDCS (as defined in the applicable Service Agreement) |
| **Address:** | As defined in the applicable Service Agreement or as otherwise provided by virtualDCS |
| **Contact person's name, position and contact details:** | For general matters: virtualDCS's Data Protection Office at:<br>Name: Malcolm Wood<br>Email: gdpr@ametrosgroup.com<br>Telephone: 0330 223 2246<br>Address: Lakeside Offices, Thorn Business Park, Hereford, England, HR2 6JT |

| | |
|---|---|
| | For security matters: virtualDCS's Information Security Office at:<br>Name: Ross Devine<br>Email: servicedesk@virtualdcs.co.uk<br>Telephone: 03453888327<br>Address: The Waterscape, 42 Leeds and Bradford Road, LS53EG. |
| **Activities relevant to the data transferred under this DPA:** | The Services |
| **Role (controller/processor):** | Processor |

## B. Description of transfer

| | |
|---|---|
| **Categories of data subjects whose personal data is transferred:** | Categories of data subjects whose Personal Data may be Processed in order to perform the Services may include, among others, Customer's customers, prospects, representatives and end users, such as Customer's employees, job applicants, contractors, collaborators, partners, suppliers, customers and clients. |
| **Categories of personal data transferred:** | Personal categories of data may include but are not limited to: Personal contact information such as name, contact information, email address; information concerning family, lifestyle and social circumstances including age, date of birth, gender; employment details including employee schedules and performance; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers; Customer IP addresses and online behaviour and interest data. Customer shall use |

| | |
|---|---|
| | reasonable efforts to limit such personal data disclosed to virtualDCS. |
| **Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:** | Based on the applicable Services, Customer's end users may disclose sensitive information that is not currently contemplated. Customer shall use reasonable efforts to limit such data disclosed to virtualDCS, which is applicable to the Services and is necessary for Processing. |
| **The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):** | Continuous or as otherwise provided in the Service Agreement. |
| **Nature of the processing:** | As required to perform the Services, and may include but is not limited to organisation, structuring, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction. |
| **Purpose(s) of the data transfer and further processing:** | For processing in Processor software solutions, support and maintenance, and development, in each case as permitted in the Service Agreement. |
| **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:** | As detailed in the Service Agreement. |
| **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:** | As permitted by the Service Agreement. In particular, transfers to hosting subprocessors may be required for storage and remote data processing, and shall be for a nature and duration as permitted by the Service Agreement. |

## C. Competent Supervisory Authority

| | |
|---|---|
| **Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 of the EU SCCs):** | UK Information Commissioners Office |

# Appendix 2

## Technical and Organisations Measures

## Overview

This document is a condensed list of the technical and organisational data security measures currently in place that protect personal data being processed by Virtual Datacentre Services.

New security measures will be added to this list as controls are implemented in accordance with the organisations wider data compliance infrastructure development strategy.

## 1. Software

**This section refers to security measures in place surrounding our computer software:**

- ✓ All software is licenced in accordance with the proper terms of use.
- ✓ Operating systems include built-in firewall security.
- ✓ Dedicated security software is active on all computer equipment.
- ✓ Security software performs on-access scanning and daily disk scans.
- ✓ Security software includes hosted firewall control.
- ✓ Security software includes malware and ransomware protection.
- ✓ Security software agents are managed by a centralised administration console.
- ✓ Email servers include built-in anti-virus and anti-spam protection.
- ✓ All unnecessary software is removed from systems.
- ✓ Sandbox systems are used to isolate software in test environments.
- ✓ Automated processes ensure high-risk and critical security updates are applied to operating systems.

## 2. Hardware

**This section refers to security measures in place surrounding our computer hardware:**

- ✓ Mobile computer equipment is protected with pre-boot authentication disk encryption.
- ✓ Mobile computer equipment is equipped with mobile device management software.
- ✓ Mobile phone devices can be remote wiped.
- ✓ Mobile phone devices are equipped with mobile device management.
- ✓ Home office equipment is protected with pre-boot authentication disk encryption.

- ✓ Home office equipment can be remote wiped.
- ✓ Old computer equipment is securely disposed of by certified processes.
- ✓ An information asset register is maintained that tracks hardware.

## 3. Firewalls

**This section refers to security measures in place that protect our networks from unauthorised access:**

- ✓ All networks are protected by a boundary firewall
- ✓ Secondary firewalls are in place that divide internal networks

## 4. User access

**This section refers to security measures that protect user accounts and access to our various systems:**

- ✓ Default passwords and user accounts are removed from equipment
- ✓ New user accounts must be authorised by an appropriate manager
- ✓ All users have unique logon accounts for each system
- ✓ User access to systems and data is restricted to what is necessary
- ✓ Minimum password complexity is enforced by technical controls

## 5. Data Backup

**This section refers to data backup processes that protect our systems and data:**

- ✓ Regular data backups of systems are maintained
- ✓ Data backups are replicated offsite to redundant servers
- ✓ The data backup process is routinely monitored
- ✓ Data restoration tests are carried out at least every 30 days

## 6. Our Online platforms

**This section refers to security measures in place surrounding online platforms that we manage:**

- ✓ Our online platforms use end-to-end encryption

- ✓ Processes are in place to ensure high-risk and critical security updates are applied to our online platform systems
- ✓ Our administrators can remote wipe devices that are synchronised with our online platforms
- ✓ Our online platforms are not hosted in, or replicated to, data centres outside of the Europe

## 7. Technical Support

**This section refers to resources that are dedicated to supporting our computer systems and networks:**

- ✓ IT Services have full remote access to support computer equipment
- ✓ Remote monitoring and management agents are active on all computer equipment
- ✓ All home office environments are supported by dedicated IT services
- ✓ All sites, regional locations, and satellite offices confirm to the same technical data security standards

## 8. Policies and Procedures

**This section refers to structured processes that are in place which guide our data protection principals:**

- ✓ A document data protection/information security plan is in place
- ✓ A documented risk management policy is in place
- ✓ A documented acceptable use of IT resources policy is in place
- ✓ A documented password policy is in place that stipulates:
- ✓ Passwords to all systems must contain at least eight to eleven characters
- ✓ Passwords must contain a mixture of upper and lower case, numbers, and special characters
- ✓ The password policy requires passwords are changed if they are believed to be compromised
- ✓ The password policy gives guidance on best practices, such as how to avoid choosing passwords based on easily discovered information and how to avoid creating inappropriate passwords
- ✓ A documented business continuity policy (disaster recovery plan) is in place
- ✓ The disaster recovery plan is tested annually to ensure its relevance
- ✓ A documented access control list is in place that shows who has access to systems and secure areas
- ✓ A documented change management policy is in place to govern how changes to the information management system are carried out

- ✓ A process is in place to record and assess data security breaches
- ✓ Guidance has been provided to our staff on how to recognise and respond to a data security breach
- ✓ A Data Protection Impact Assessment process (DPIA) is in place for reviewing high-risk data processing activities

## 9. Training

**This section refers to how we minimise data security risks from human error:**

- ✓ All staff are provided with basic data security awareness training
- ✓ Staff are required to repeat data security awareness training at least annually
- ✓ Individual assessments are carried out on training requirements for staff with specific roles

## 10. Certification

**This section lists the accreditations we have gained in the field of data protection and security:**

**We have the following professional accreditations:**

- ✓ Cyber Essentials – Protection from online threats
- ✓ ISO 27001 – Information Security Management

## 11. Physical Security

**This section refers to security measures in place surrounding our office-based activities:**

- ✓ Site security risk assessments are carried out in our offices and other facilities
- ✓ Paper-based records are securely destroyed when no longer needed

## Disclaimer

To the best of our knowledge, the information contained herein is accurate and reliable.