

GoAssetWorks Limited

G-Cloud 13May 2022

SaaS Terms and conditions

May 13, 2022

SOFTWARE AS A SERVICE AGREEMENT

This Software as a Service Agreement (“Agreement”) is effective , 20 (“Effective Date”) and entered into between GoAssetWorks Limited (“AssetWorks”), located at 10 Finsbury Square, London, England, EC2A 1AF and (“Customer”), a , located at . In consideration of the mutual covenants contained herein, the parties agree as follows:

Overview

This is a Software as a Service cloud-based distribution model that delivers turnkey software applications, hosting and support as a combined service provided by AssetWorks under this Agreement (collectively the “SaaS”). This Agreement describes the respective responsibilities of the parties and the service levels. This Agreement incorporates the following Schedules that shall be considered an integral part of this Agreement:

- Schedule 1 Solution Packages
- Schedule 2 Hosting Services
- Schedule 3 Maintenance & Support
- Schedule 4 Professional Services
- Schedule 5 Fee Schedule
- Schedule 6 Data Processing Agreement (“DPA”)

1. Software as a Service, Maintenance and Professional Services

- A. Software as a Service.** In consideration of the fees paid by Customer under this Agreement, AssetWorks will provide Customer with access, through a website or designated IP address, to specific components in its proprietary software (“Software”) hereunder listed on Schedule 1, in an isolated, single-tenant environment, which is maintained by AssetWorks in a hosted environment at a third-party data center (“Hosting Services”), as set forth in Schedule 2.
- B. Maintenance.** AssetWorks will provide (i) online and telephone support relating to the use of the SaaS and (ii) updates, enhancements and modifications to the Software as they are developed and made generally available (“Maintenance and Support”), as set forth in Schedule 3.
- C. Services.** Subject to the payment of Service fees, AssetWorks will provide Customer with training, consultation, and other related services (“Professional Services”), as set forth in Schedule 4.

2. Rights and Permitted Use

- A. Right of Use Grant.** Subject to the terms and conditions of this Agreement, AssetWorks grants to Customer a non-exclusive and non-transferable right for Authorised Users to access and use the ReADY, AiM and Go Software, and Documentation for Customer’s internal business operations. “Authorized Users” means Customer’s employees or independent contractors working within their job responsibilities or engagement by Customer or other end user for which AssetWorks has granted Customer the right to use the SaaS. “Documentation” means documentation in the form of instructions, videos, digital curriculum and manuals provided by AssetWorks electronically, that describes the function and use of the SaaS. The Customer may copy, in whole or in part, any printed material relative to the Software that may be provided by AssetWorks under this Agreement. Additional copies provided by AssetWorks will be billed to Customer at AssetWorks’ standard rates.

- B. Restrictions.** Except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties, Customer will not (i) directly or indirectly decompile, disassemble, reverse engineer, or otherwise attempt to discover the source code or underlying structure, ideas, know-how or algorithms relevant to the SaaS, Software, Documentation, or any data related to the SaaS; (ii) copy (excluding Customer backup rights), modify, enhance, translate, change the data structures for or create derivative works from, the SaaS; (iii) rent, lease, sell, or otherwise provide access to the SaaS to any third-party or to anyone other than Customer's Authorized Users; (iv) interfere with or disrupt the integrity or performance of the SaaS or third-party data contained therein; or (v) attempt to gain unauthorised access to the SaaS or its related systems or networks.
- C. Customer Data.** Customer shall retain all right, title, and interest in and to the data entered or submitted by Customer by means of the SaaS ("Customer Data"). Customer grants to AssetWorks a royalty-free, non-exclusive, non-transferable license for the term of this Agreement to use Customer Data to the extent necessary to perform its obligations under this Agreement. Notwithstanding anything to the contrary, AssetWorks shall have the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the SaaS and related systems and technologies (including, without limitation, information concerning Customer Data and data derived therefrom), and AssetWorks will be free (during and after the term hereof) to (i) use such information and data to improve and enhance the SaaS and for other development, diagnostic and corrective purposes in connection with the SaaS and other AssetWorks offerings, and (ii) disclose such data solely in aggregate or other de-identified form in connection with its business which includes but not limited to anonymized institutional and transactional data for use in its sales, marketing and training material and/or demonstrations.

3. Term

The Term of the Agreement shall commence as of the Effective Date and shall continue for three (3) years ("Initial Term") unless terminated earlier as set forth below.

At the end of the Initial Term, the Agreement shall automatically renew for successive one-year terms, unless or until either party provides the other party with written notice of non-renewal at least ninety (90) days prior to the end of the then current term. If such notice is provided, then the Agreement will automatically terminate at the end of the then current term.

4. Fees and Payments

- A. Customer shall pay AssetWorks the applicable fees as set forth in Schedule 5. The Annual Service Fee will increase five (5) % on each anniversary during the Initial Term, and every successive one-year renewal term.
- B. Customer shall be responsible for all taxes and charges assessed or imposed with respect to amounts payable hereunder, exclusive of VAT which shall be added to AW's invoices at the appropriate rate.
- C. If Customer wishes to make monthly payments by credit card all to which such transaction constitutes a credit card charge, an additional credit card processing transaction fee will be calculated at four and one half (4.5)%.
- D. AssetWorks shall invoice Customer annually, in advance, and all invoiced fees shall be due and payable within thirty (30) days of the date of an invoice. All payments shall be made without deduction for any taxes or withholding or other offset.
- E. Any amounts not paid when due will be subject to interest accrued at the rate of eight (8) % per annum above the base rate from time to time of Barclays Bank plc or, if lower, at the maximum rate permitted

under the Late Payment of Commercial Debts (Interest) Act 1998 and Late Payment of Commercial Debts Regulations 2002 and 2013, which interest will be immediately due and payable from the due date for payment until the date of actual receipt of the amount in cleared funds by AssetWorks. Interest payments that are accrued during billing disputes should be credited back to the Customer if said dispute is found to be through no fault of the Customer.

- F. A Customer will be considered delinquent if payment in full is not received forty-five (45) days from the date of the invoice. AssetWorks reserves the right to suspend any Service including Customer's access to the SaaS if the Customer account becomes delinquent and is not cured within ten (10) days of written notice from AssetWorks. Customer will continue to be charged and hereby agrees to pay for SaaS during any period of suspension. Customer's failure to pay any invoice after this ten (10) day period shall constitute a material default hereunder and shall entitle AssetWorks, without any additional notice, to terminate the Agreement.
- G. Following the expiry of three (3) years from the Initial Term, the Customer may terminate this Agreement by giving not less than ninety (90) days' written notice to AssetWorks at any time. Such termination to be with effect on and from the next anniversary date of this Agreement following the expiry of the period of ninety (90) days from the date of AssetWorks receipt of that termination notice.

If this Agreement is not terminated in accordance with this clause, in addition to all amounts due and payable for Services rendered up through the effective termination date, Customer will be responsible for the payment of 25% of full amount payable till the following anniversary date ("Cancellation Charges").

If Customer decides to terminate the Agreement within the first two years of the Initial Term, or services have been terminated by AssetWorks for breach of contract within the Initial Term, Customer will be responsible for the payment of Cancellation Charges. Cancellation Charges shall also apply if this Agreement is terminated within the last 90 days of the Initial Term. These Charges will be invoiced as a single charge and are payable within our terms included in Agreement.

In no event shall the termination relieve Customer's obligation to pay any fees payable to AssetWorks for the period prior to the effective renewal date.

5. Ownership of Software and Data

Customer shall not obtain any ownership rights, title or interest in the software, hardware or systems developed or employed by AssetWorks in providing Services under the Agreement. AssetWorks shall not obtain any ownership rights, title or interest to Customer's data files. Upon expiration or termination of the Agreement for any reason, AssetWorks agrees to provide Customer with a copy of Customer's data files, as they exist at the date of expiration or termination. Nothing contained herein is intended to modify the Customer's rights under any separate license agreement between Customer and AssetWorks. For avoidance of doubt, Customer shall not obtain ownership or any other rights, title or interest in the Solutions referenced in Schedule 1 either during the Term of this Agreement or after the termination of this Agreement.

6. Intellectual Property Rights

- A. Customer acknowledges and agrees that the Software consists of proprietary source code developed and owned by AssetWorks, as well as contributions made by third parties whose source code ("Third-Party Software") is incorporated into and made a part of the Software.
- B. AssetWorks owns all intellectual property rights in and to: (i) the SaaS; (ii) the Software; (iii) all updates, enhancements and modifications to the Software and SaaS; (iv) any Documentation or data related to the SaaS; and (v) any software, applications, inventions, or other technology developed in connection with the

Software or the SaaS. Customer obtains no rights, title or interest in the Software, SaaS, or Documentation and only is permitted a license to use the Software and SaaS as expressly provided in this Agreement.

- C. Neither party grants to the other party under this Agreement any actual or implied license to use its trademarks, trade names, service marks, copyrights, logos, markings, or other brand designations.

7. Confidentiality

- A. Each party acknowledges it may have access to confidential information of the other party. "Confidential Information" shall mean any information relating to trade secrets, data, designs, drawings, documentation, software (regardless of form or media), prototypes, processes, methods, concepts, research, development, facilities, employees, vendors, clients, marketing, financials, business activities, and other similar information whether obtained or disclosed orally or in writing. To the extent practicable, the disclosing party shall mark and/or identify Confidential Information as confidential or proprietary at the time of disclosure; provided however, the obligation of Confidentiality shall also apply to information which, based on its nature, is reasonably expected to be deemed confidential.
- B. Confidential Information shall not include information that: (i) becomes generally available to the public through no fault of the receiving party; (ii) is lawfully provided to the receiving party by a third-party not under an obligation of confidentiality; (iii) was lawfully possessed by the receiving party prior to receiving the Confidential Information from the disclosing party, as evidenced by the receiving party's records; or (iv) the receiving party can demonstrate was independently developed by receiving party without use of the disclosing party's Confidential Information. The receiving party agrees it will not disclose Confidential Information to any third-party without the prior written consent of the disclosing party.
- C. The receiving party will limit access to the Confidential Information to its directors, officers, employees, agents, advisors, and contractors who (i) have a need to know the Confidential Information in connection with the Purpose, (ii) are bound to confidentiality obligations no less restrictive than those set forth herein, and (iii) have been informed of the confidential nature of such information. The receiving party shall protect the Confidential Information from unauthorised use, access, or disclosure in the same manner as it protects its own confidential and proprietary information of a similar nature, and, in any event, with at least a reasonable degree of care.

8. Warranty Disclaimer/Limitation of Liability

- A. AssetWorks represents that it has the right to grant right of use of the Software to Customer as provided in Section 2. During the warranty period as defined in 8 D, AssetWorks further warrants that the Software will conform to the specifications published by AssetWorks or provided by AssetWorks to Customer in the Documentation. In the event the Software fails to conform to the Documentation, AssetWorks' sole obligation shall be to correct the errors in accordance with the provisions of this Section 8 D.
- B. AssetWorks will defend, at its own expense, any action brought against Customer to the extent that it is based on a claim that the AssetWorks Software infringes a patent or copyright, and AssetWorks will pay those costs and damages finally awarded against Customer in any such action that are attributable to any such claim, but such defense and payments are conditioned on the following: (i) that AssetWorks shall be promptly notified in writing by Customer following its receipt of any such claim; (ii) that AssetWorks shall have sole control of the defence of any action on such claim and all negotiations for its settlement or compromise; (iii) should the Software become, or in AssetWorks' opinion is likely to become, the subject of a claim of infringement of a patent or copyright, then Customer shall permit AssetWorks, at its option and expense, either to (i) procure for Customer a non-infringing license to use the Software; (ii) modify the Software so that it becomes non-infringing; (iii) procure for Customer a depreciated credit for the Software and accept its return. Depreciation shall be an equal amount per year from the date of receipt of the

Software, which the parties agree shall be three (3) years. AssetWorks shall have no liability to Customer under any provision of this clause with respect to any claim of patent or copyright infringement that is based on Customer's unauthorised use or combination of the Software with software or data not supplied by AssetWorks as part of the Software.

- C. Customer agrees to defend and hold AssetWorks harmless against any claims made by any third-party against AssetWorks arising out of Customer's use of the Software unless such claims are due to the negligence or wilful misconduct of AssetWorks.
- D. The warranty period for the Software shall extend for a period of ninety (90) days from the date of delivery of the Software. During the warranty period, in the event that the Customer encounters an error and/or malfunction whereby the Software does not conform to the description in the Documentation, AssetWorks will respond as follows:
 - i. In the event that, in the mutual and reasonable opinion of AssetWorks and the Customer, there exists an error or nonconformance to the Documentation, AssetWorks will take such steps as are required to correct the error with due dispatch.
 - ii. In the event that, in the mutual and reasonable opinion of AssetWorks and the Customer, the error or nonconformance to the Documentation does not constitute a serious impediment to the normal intended use of the Software, AssetWorks will correct the error and distribute the correction to the Customer in accordance with AssetWorks' normal Software revision schedule.
- E. AssetWorks does not warrant third-party software. Warranties, if any, for third-party software is passed through to Customer.
- F. All other conditions, warranties or other terms which might have effect between the Parties or be implied or incorporated into the Agreement or any collateral contract, whether by statute, common law or otherwise, are hereby excluded, including the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or the use of reasonable skill and care. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY ASSETWORKS, ITS AGENTS OR EMPLOYEES SHALL CREATE ANY ADDITIONAL REPRESENTATIONS, ASSURANCES, WARRANTY, OR IN ANY WAY INCREASE THE SCOPE THIS AGREEMENT. SUCH WARRANTIES SHALL NOT BE DEEMED TO HAVE FAILED OF THEIR ESSENTIAL PURPOSE SO LONG AS ASSETWORKS IS MAKING GOOD FAITH EFFORTS TO CORRECT DEFECTS OR FAILURES UNDER THE TERMS OF THE WARRANTY. NEITHER ASSETWORKS NOR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE ASSETWORKS SOFTWARE SHALL BE LIABLE FOR ANY CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT OF THIS AGREEMENT OR THE USE OF OR INABILITY TO USE THE ASSETWORKS SOFTWARE EVEN IF ASSETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- G. IN NO CASE SHALL ASSETWORKS' AGGREGATE LIABILITY FOR ALL MATTERS ARISING OUT OF THE SUBJECT MATTER OF THIS AGREEMENT, WHETHER IN CONTRACT, NEGLIGENCE, TORT OR OTHERWISE, EXCEED THE AMOUNT ACTUALLY RECEIVED BY ASSETWORKS PURSUANT TO THIS AGREEMENT DURING THE PREVIOUS TWELVE (12) MONTH PERIOD. THE PARTIES AGREE TO THE FOREGOING LIABILITY RISK ALLOCATION. ANY CLAIM BY CUSTOMER AGAINST ASSETWORKS RELATING TO THIS AGREEMENT MUST BE MADE IN WRITING AND PRESENTED TO ASSETWORKS WITHIN SIX (6) MONTHS AFTER THE DATE ON WHICH THIS AGREEMENT EXPIRES OR IS OTHERWISE TERMINATED.

9. Termination

- A. Except as otherwise provided in Section 4. F. of this Agreement, a default shall occur if: (i) a party fails to perform any of its material obligations under the Agreement and such failure remains uncured for thirty

(30) days after receipt of written notice thereof; or (ii) a party ceases to conduct business, becomes or is declared insolvent or bankrupt, is the subject of any proceeding relating to its liquidation or insolvency which is not dismissed within ninety (90) days or makes an assignment for the benefit of creditors.

- B. If default occurs, the non-defaulting party, in addition to any other rights available to it under law or equity, may withhold its performance hereunder or may terminate the Agreement by written notice to the defaulting party. Unless otherwise provided in the Agreement, remedies shall be cumulative and there shall be no obligation to exercise a particular remedy.
- C. Upon termination of this Agreement, whatever the reason, the Documentation and any copies thereof made by Customer pursuant to this Agreement shall be returned to AssetWorks.
- D. Upon termination of this Agreement, AssetWorks will terminate Customer's access to Solutions referenced in Schedule 1. All hosting, maintenance, and support as set forth in Schedules 2 and 3 shall terminate on the same date.

10. Third-Party Integration

Customer acknowledges that Customer may need to obtain additional third-party technology ("Third Party-Technology"). Customer agrees that the rights and licenses with respect to Third-Party Technology shall be under a separate purchase, license or services agreement by and between the Customer and the vendors of such Third-Party Technology. Customer shall comply with the applicable purchase and/or license agreement with respect to any Third-Party Technology. Any amounts payable to any such vendors shall be the Customer's responsibility and Customer assumes all risks and liabilities to third-party vendors.

11. Assignment

This Agreement shall not be assignable by Customer without AssetWorks prior written consent, and any attempted assignment without such consent shall be void. No assignment of this Agreement shall be valid until and unless consented to in writing by AssetWorks and assumed by the assignee in writing. When duly assigned in accordance with the foregoing, this Agreement shall be binding upon and shall inure to the benefit of the assignee.

12. Privacy

The parties must comply with the requirements of the any privacy law in the country in which the party (and/or the individual about whom the personal information relates) is located, and in any country to which the personal information is to be sent; and only use, manipulate, store and handle personal information for the purposes of meeting its obligations under this Agreement and pursuant to the Data Processing Agreement attached as Schedule 6.

13. Entire Agreement

This Agreement sets forth the sole and entire understanding between AssetWorks and Customer and supersedes all prior proposals, oral or written, all previous negotiations and all other communications or understandings between AssetWorks and Customer with respect to the subject matter hereof. It is expressly agreed that if Customer issues a purchase order or other document for the services provided under this Agreement, such instrument will be deemed for Customer's use only, and any provisions inconsistent with this Agreement shall have no effect.

whatsoever upon this Agreement. No amendments to this Agreement, either at the execution or subsequently, shall be binding on AssetWorks or Customer unless agreed to in writing by both parties.

14. Governing Law

The Agreement and any disputes or claims arising out of or in connection with its subject matter or formation shall be governed and construed in accordance with the laws of the England and Wales without regard to choice of law principles and the courts of England and Wales shall have exclusive jurisdiction in respect of the same.

15. Severability

If any provision of the Agreement is held by a court of competent jurisdiction to be invalid, void or unenforceable, the remaining provisions shall nevertheless continue in full force without being impaired or invalidated in any manner.

16. Force Majeure

Neither party shall in any circumstances be in breach of this Agreement nor liable for any delay in performing, or any failure to perform, any of its obligations under this Agreement (excluding a Customer's payment obligations) if such delay or failure results an event, or a series of related events, that is outside the reasonable control of the party affected (including without limitation failures of or problems with the internet or a part of the internet, hacker attacks, virus or other malicious software attacks or infections, power failures, industrial disputes affecting any third party, changes to the law, disasters, explosions, fires, floods, pandemics, riots, terrorist attacks and wars).

17. Waiver

No provision of the Agreement may be waived unless in writing, signed by both of the parties hereto. Waiver of default of any provision of the Agreement shall not operate or be construed as a waiver of any subsequent default of such provision, nor shall a waiver of any one provision of the Agreement be deemed to be a waiver of any other provision.

18. Notices

All notices under this Agreement will be in writing and will be delivered by personal service, facsimile, e-mail or certified mail, postage prepaid, or overnight courier to such person and address as may be designated from time to time by the relevant party, which initially shall be the address set forth in the signature block below. A notice delivered by hand is deemed to have been received when delivered (or, if delivery is not in business hours, 9:00 A.M. GMT on the first business day following delivery). A correctly addressed notice sent by prepaid first-class post or recorded delivery post shall be deemed to have been received at the time at which it would have been delivered in the normal course of post. An e-mail shall be deemed to have been delivered within twenty-four (24) hours from the time of being sent, provided that no "non-deliverable" notice is received by the sender.

19. Headings

The Section headings in the Agreement are inserted only as a matter of convenience, and in no way define, limit, or extend or interpret the scope of the Agreement or of any particular Section.

20. Authorization

Each of the parties represents and warrants that the Agreement is a valid and binding obligation enforceable against it and that the representative executing the Agreement is duly authorised and empowered to sign the Agreement.

21. Dispute Resolution

The Parties will attempt to resolve any dispute arising under or relating to the Agreement through informal means. At the written request of either party, the Parties will submit the dispute to senior management representative for each Party for review and resolution. Should the dispute not resolved in thirty (30) days of the written request and the Parties do not both agree to an extension, the Parties agree that the dispute between them shall be referred to a mediator, who will be selected by mutual agreement for resolution by mediation. The costs of mediation shall be equally shared between the Parties. If a dispute is not settled within 7 days of the mediation being instituted, or within such other period as the Parties shall agree in writing, the dispute(s) shall then be referred to and finally resolved by binding arbitration under the Arbitration Act 1996. All costs will be added to the arbitration claim for the Arbitrator to award as the Arbitrator deems appropriate.

22. Relationship of Parties

The relationship of the parties shall at all times be one of independent contractors. Nothing contained herein shall be construed as creating any agency, partnership or other form of joint enterprise between the parties.

23. Conflicting Provisions

This Agreement and all of the exhibits, schedules, and documents attached hereto are intended to be read and construed in harmony with each other, but in the event any provision in any attachment conflicts with any provision of this Agreement, then this Agreement shall be deemed to control, and such conflicting provision to the extent it conflicts shall be deemed removed and replaced with the governing provision herein.

24. Counterparts

The Agreement may be executed simultaneously in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

25. Third-Party Beneficiaries

This Agreement does not create, and shall not be construed as creating, any rights or interests enforceable by any person not a party to this Agreement.

SIGNATURES

IN WITNESS WHEREOF, the parties have executed this Agreement through their duly authorised representative(s).

AssetWorks

Name: _____

Title: _____

Sign: _____

Date: _____

Notice Address:
2441 Nacogdoches Road
PMB 535
San Antonio, Texas 78217
Att: Mindy Payne
mindy.payne@assetworks.com

Telephone (210) 301-1701

Fax (210) 301-0298

Customer

Name: _____

Title: _____

Sign: _____

Date: _____

Notice Address:
INSERT ADDRESS

Telephone: **INSERT PHONE**

FAX: **INSERT FAX**

SCHEDULE 2. HOSTING SERVICES.

OVERVIEW

AssetWorks uses data centers, including but not limited to Amazon Web Services (“Data Center”) to provide hosting services and related support to customers that wish to outsource the operation and maintenance of computer applications listed in Schedule 1. This Schedule describes the services to be provided by AssetWorks the respective responsibilities of the parties, and the service levels.

SERVICES

AssetWorks will perform the services as described in the Scope of Hosting Services (“Services”).

The general scope of services addressed by this Schedule includes the operation, maintenance, and support of the:

- Database software for the Applications hosted under this Agreement
- Database security
- Data Center

The Services specifically excludes operation and maintenance of the following:

- Customer hardware, including Customer’s servers, printers, network hardware (including routers and switches) and other Customer site computing equipment;
- Customer application software other than noted in Schedule 1;
- Customer Local Area Networks (“LAN”); and
- Customer network infrastructure for connecting to the Internet and to the Data Center.

CUSTOMER RESPONSIBILITIES

The Customer is responsible for:

- Assigning a primary and alternate Customer representative to coordinate all communications and activities related to AssetWorks services.
- Providing user identification data and determining the appropriate security profile for each user. Customer will control security at the Application level.
- All printing. No print job will print at the Data Center and all physical printing requirements will be handled by the Customer.
- The purchase and installation of printers at Customer’s sites for the Application being utilized as defined in Schedule 1.
- Installation, operation and maintenance of all workstation software (and Customer’s LAN, existing data communications configuration, hardware, or software required at the Customer’s site. AssetWorks network and network responsibility extends from the Data Center routers at Data Center to all connected equipment at Data Center.
- Testing updates and fixes applied by AssetWorks to Applications used by Customer. With the exception of emergency fixes, Customer will test updates and fixes prior to their introduction to the Production environment within a mutually agreed upon time frame.
- Testing upgrades. Upgrades will be moved to production by the AssetWorks at the end of the Customer testing period unless specific problems are documented in writing to AssetWorks.

- Diligent analysis of suspected problems to determine their specific nature and possible causes before calling the AssetWorks for assistance. Notwithstanding this diligence requirement, Customer is responsible for informing AssetWorks of any problems encountered in a timely manner.

SCOPE OF HOSTING SERVICES

All of the services, functions, processes, and activities described below will be collectively described as the “Services” for purposes of this Schedule. All Services will be provided by AssetWorks to and for the Customer’s benefit in a manner that will meet the objectives outlined in this Schedule.

Software

Support Software includes the Application Instances as defined below, operating system, utilities, database software, and all necessary licenses required to operate the Application and provided by AssetWorks as part of the Services.

Infrastructure

All infrastructure; e.g., servers, is physically located in the [United Kingdom or Ireland, depending on the geographic location of the Customer]. Sufficient resources; e.g., bandwidth, disk space, CPU, VPN tunnels, for typical production and non-production deployments are included. In the event additional resources are required the following rates apply:

- AssetWorks provides 250 GB of bandwidth (outgoing/month). Customer agrees to pay £100/month for every additional 100 GB of data transfer(out) in excess of the amount included in the monthly recurring fee for bandwidth contracted under above pricing model.
- AssetWorks provides a standard allotment of 100GB for document repositories/data repositories. Additional resources can be purchased in 100GB increments for an additional £250/month each.

Application Instances

AssetWorks will maintain a single production Application Instance. The production Application Instance will provide the daily, real-time transaction data to the Application users.

In addition to the Production Application Instance, AssetWorks will maintain one additional, non-production application instance, the Test Application Instance. Upon request by Customer, AssetWorks will refresh the Test Application Instance with Customer’s Production data up to 4 times throughout the calendar year at no additional cost.

Backups

Full database and incremental file system backups are taken each night and stored at an offsite facility. Backup data is retained for ten (10) days. Customer may request, at no additional charge, one backup of the databases once per quarter, not to exceed four times per year. Each additional change request will incur a 2-hour Technical Services engagement at the contracted hourly rate.

VPN Access to the Hosted Database

One site to site VPN tunnel is allotted with two IP address configurations. AssetWorks will provision Customers with read-only access to the Database. Each additional change request will incur a 2-hour Technical Services engagement at the contracted hourly rate.

Hours of System Operations

The Application will be accessible and available to the Customer and capable of any and all normal operating functions 24 hours a day, seven (7) days a week except for periods of Scheduled Maintenance and previously approved outages. AssetWorks will not be held responsible for inaccessibility arising from communications problems occurring anywhere beyond the Amazon Web Services side of the router resident at the Data Center, nor will these hours of unavailability be counted as unavailable. Standard Support hours are Monday to Friday 8:00am to 6:00pm GMT, excluding public holidays in England. After-hours support is only available for connectivity or system inaccessibility issues and can be reached at 02030482926 Option: 4.

Maintenance in Data Center

Customer agrees to be responsible for maintaining and updating the authorized contact list with AssetWorks (Customer Care). AssetWorks will not be held responsible for maintenance notifications missed due to out-of-date Authorized Contact information.

Planned Maintenance

AssetWorks will complete routine maintenance on the Application on a monthly basis. The maintenance schedule will be published and provided to the Customer's Authorized Contact. AssetWorks will provide at least 14 day notice to any changes in the published maintenance schedule.

Unplanned Maintenance

If AssetWorks is required to perform additional maintenance outside of the scheduled maintenance window, AssetWorks will use reasonable efforts to provide Customer with prior (written) notice of said "unplanned maintenance" (except for emergency maintenance) and Customer agrees to use reasonable efforts to comply with any maintenance requirements requested by AssetWorks. With written notification of "unplanned maintenance" and agreement from Customer, SLAs will not apply during unplanned maintenance.

Emergency Maintenance

AssetWorks reserves the right to perform emergency maintenance as needed outside the scheduled maintenance. In such event, AssetWorks will make a reasonable effort to notify the Customer, if feasible, under the circumstances. Any such maintenance will be considered an "Emergency Maintenance". SLAs will apply during Emergency Maintenance.

Application Maintenance. In addition to AssetWorks maintenance in the Data Center, Customer is entitled to additional maintenance and support as set forth in a separate agreement between the parties.

Service Level

This Service Level Agreement ("SLA") is intended to provide an understanding of the level of service to be delivered by the AssetWorks for the Services specified in this Schedule. The service levels set forth below apply to the Services provided by AssetWorks under the Agreement.

Availability

AssetWorks will use commercially reasonable efforts to provide Services with an average of 95% Availability (as such term is hereinafter defined) for each quarter during the Term. For purposes of the Agreement, “Availability” during any quarter refers to an Authorized User’s ability to log into the Application during such quarter, and will be calculated in accordance with the following formula:

$$x = (y - z) / y * 100$$

Where,

- “x” is the Availability of the Application during the quarter;
- “y” is the total number of hours in such quarter minus the number of hours during such quarter that the Customer is unable to log into the Application because of (a) regularly scheduled maintenance windows for the Application and for times in which Customer has been notified in writing (including e-mail) by AssetWorks in advance thereof; (b) a Force Majeure Event; (c) non-performance of hardware, software, ISP connections, and other equipment that is not provided by AssetWorks or certified by AssetWorks for use in conjunction with the Services (except as such non-performance is directly or indirectly caused by AssetWorks).
- “z” is the number of hours in such month during which the Customer is unable to log into the Application (other than for reasons set forth in the definition of “y” above); provided that AssetWorks has been notified or is otherwise aware (or reasonably should be aware) of Customer’s inability to utilize the Application.

Fee Adjustment

In the event that AssetWorks does not meet the Availability levels set forth below, the amount of fees payable by Customer will be reduced as follows:

In the event the average Availability for the Application is less than ninety five percent (95%) during any two consecutive quarters, Customer will receive a credit to its account with AssetWorks of five percent (5%) of the amount of a quarter’s aggregate Services Fees paid or payable by Customer to AssetWorks. Custom reports, scripts, action codes, web services or other interfacing programs causing the inability to log into the application will not be considered downtime for the purpose of the availability calculation.

AssetWorks’ obligation to provide Customer with fee adjustments as specified above is conditioned on Customer providing detailed written notice to AssetWorks of its contention that AssetWorks was unable to meet the applicable Availability levels. Upon receipt of such notice, AssetWorks shall have thirty (30) days to investigate the contention. If, at the end of the thirty (30) day period it is determined that AssetWorks did in fact fail to meet the applicable Availability levels, Customer will receive the appropriate credit to its account during the next invoice cycle.

The remedies set forth in this Section of this Schedule shall be Customer’s sole remedy and AssetWorks’ entire liability in the event of a breach of this Service including the failure of any Availability measurements to meet the thresholds specified above.

SCHEDULE 3. SOFTWARE MAINTENANCE AND SUPPORT.

OVERVIEW

AssetWorks support and maintenance rapidly resolves technical issues, provides high-quality customer service, gives you access to the latest versions of software, and offers a wealth of valuable benefits.

This Schedule describes the services to be provided by AssetWorks the respective responsibilities of the parties, and the service levels.

Correction of Deviations

In the event that the Customer encounters an error and/or malfunction ("Deviation") in the Software, it shall communicate the circumstances and any supporting information to AssetWorks. Upon receipt, AssetWorks will respond as follows:

- a. In the event that, in the mutual and reasonable opinion of AssetWorks and the Customer, there exists a Deviation that does not constitute a serious impediment to the normal intended use of the Software, AssetWorks may correct the Deviation and distribute the correction to the Customer in accordance with AssetWorks' normal Software revision schedule;
- b. In the event that, in the mutual and reasonable opinion of AssetWorks and the Customer, there exists a Deviation that does constitute a serious impediment to the normal intended use of the Software, AssetWorks will take such steps as are required to correct the Deviation with all due dispatch. Corrections will be applied and distributed to the latest software release. AssetWorks will have no obligation to provide development support for an issue that can be resolved by Customer installing a revision to the software.
- c. AssetWorks may in its sole discretion investigate issues related to Third-Party Software, but AssetWorks has no obligation to remedy or to pursue any workaround to any such defects, deviations or breaking changes introduced by Third-Party Software or Third-Party Technology.

Software Revisions

The Software may be revised by AssetWorks as a result of the correction of Deviations and/or the release of upgrades or improvements or modifications designed to improve the performance of the Software and/or to increase the capabilities of the Software (hereafter "Revisions"). Revisions shall be of two kinds:

- a. Revisions that the Customer is obliged to implement ("Mandatory Revisions");
- b. Revisions that may be implemented by the Customer at its option ("Optional Revisions").

AssetWorks currently offers 3 planned releases/updates per year. No charge shall be made to the Customer for either Mandatory Revisions or Optional Revisions.

Customer shall update the Software at least once annually with a major release (excluding patches and minor revisions).

All Software must be within one (1) major version from the latest major release. For example, a major version is identified as (X4.01) and minor is (X4.01.01). Customer shall accept all minor versions. AssetWorks will only support one prior major version behind the latest major update of the Software.

Telephone Hotline Assistance

AssetWorks, at its expense, shall make available technically qualified personnel to respond to all reasonable telephone requests that may be made by the Customer relating to the application and operation of the Software.

Technical Literature

AssetWorks shall make available to the Customer all technical literature that is considered by AssetWorks to be relevant to the Software and its use within the scope of Customer's operations.

Transmission

All Revisions and new releases (software distributions) will be transmitted to the Customer via FTP or other suitable media, at the option of AssetWorks. The Customer shall be solely responsible for mounting the software distribution and executing the appropriate instructions in order to transfer the Revisions or new releases onto its system.

Exclusions

Unless otherwise agreed in the Statement of Work, no customized solutions, e.g., transformative logic for system integrations, whether created by the Customer, a third-party or AssetWorks are included within the AssetWorks obligations under this Schedule or the Agreement.

Proper Use

- a. The Customer agrees that all reasonable effort shall be taken to ensure that neither the Software nor data files are misused.
- b. In the event that the Customer misuses the Software or data files, correction of the situation will be at Customer's expense.
- c. In the event that diagnostic assistance is provided by AssetWorks, which, in the reasonable opinion of AssetWorks and the Customer, relates to problems not caused by a Deviation in the Software, such assistance shall be at the Customer's expense.

Customizations

AssetWorks may remotely access the Software for the purpose of remote diagnostics and support.

SCHEDULE 4. PROFESSIONAL SERVICES.

Scope of Services

AssetWorks will perform the professional services (“Services”) and deliver (“Deliverables”) described in the Statement of Work (“SOW”). During the term of this Agreement, Customer may request changes in the SOW. However, any such change, including technical requirements, schedule, or any increase or decrease in the compensation due to AssetWorks, shall be prosecuted in accordance with Section 4 of this Schedule and requires the mutual agreement of the parties. Said change shall be effective when incorporated by written amendment into the SOW or this Agreement.

1. Place of Performance

Unless otherwise provided in a SOW, AssetWorks may perform the Services in whole or in part at AssetWorks' place of business, Customer's place of business, and/or such other locations as AssetWorks selects.

2. Project Responsibilities

The implementation process is interactive and intensive, and success requires close teamwork between Customer and AssetWorks.

AssetWorks Responsibilities

The work performed by AssetWorks and their employees will be done in a professional manner and at a level of competence equal to the general level of competence of their profession in the industry and that the applications that they develop will perform and work correctly.

- AssetWorks will assign a “Implementation Specialist” to oversee the implementation. The Implementation Specialist has responsibility for AssetWorks tasks.
- AssetWorks will maintain implementation continuity from phase to phase for the complete project. The Implementation Specialist will be the primary single point of contact for all issues. Customer will likewise assign a primary point of contact for all communications during the project. Continuity by AssetWorks will be assured through the supervisory involvement of the Program Manager.
- Customer expects AssetWorks to drive the tasks required to meet the project requirements as defined in the SOW.

Customer Responsibilities

- Customer will actively participate in implementation activities and apply necessary resources to complete tasks that are assigned to the Customer.
- Customer will ensure that the required institutional data are loaded into templates provided by AssetWorks, scrubbed, and delivered in a timely manner, in accordance with the project schedule. Delays may affect overall costs and timeline for this project.

- Any data that cannot be loaded from the AssetWorks-provided templates due to data anomalies or faulty data is the Customer's responsibility to load manually.
- Customer is responsible for: adding new AiM users to support the products being implemented as part of this SOW, and the addition or modification of AiM user WorkDesks to support the products being implemented as part of this SOW.
- Customer is responsible for any live training sessions with their end users.

3. Project Standards

- Actual start and completion dates will be determined during the implementation planning session and adjust during the course of the project as necessary, assuming such changes are mutually agreed upon.
- This is a time & materials services effort. Times indicated for implementation support, are based on the current understanding of Customer's requirements and may be adjusted during implementation as required and such adjustments shall be coordinated between the Customer and AssetWorks. Any change to the scope of the project not contained in this SOW will be subject to the Change Order process described in Section 4 below.
- Customer will go-live with the most recent version of AssetWorks that has been released at the time of the official project kick-off meeting.

4. Changes

- (a) Issuance of Change Orders.** The Customer may, at any time by a written Change Order, make changes consistent with this Schedule and/or make changes outside the SOW, if mutually agreed by the parties in advance. Such changes may include revisions to Services or Deliverables. All Change Orders shall be subject to requirements and limitations of the applicable law.
- (b) AssetWorks' Response.** AssetWorks shall respond in writing to a Change Order issued by the Customer within thirty (30) days of receipt, advising the Customer of any impact on the costs, resources, and/or implementation schedule. If there is a cost increase or change in schedule attributable to a Change Order, AssetWorks shall so notify the Customer in writing. The Customer shall accept or reject AssetWorks' response within thirty (30) days of receipt. Failure of the parties to agree to an equitable adjustment shall relieve AssetWorks of any obligation to act upon a Change Order.
- (c) AssetWorks identified Change.** In the event that AssetWorks determines that a Customer action or inaction results in or necessitates a change that may have an impact on the costs, resources and/or implementation schedule, AssetWorks will notify Customer as soon as reasonably possible. Within twenty (20) days after said notice AssetWorks shall provide Customer with a proposal that addresses the change and its impact on the costs, resources and/or implementation schedule for Customer to accept or reject. The Customer shall accept or reject AssetWorks' response within thirty (30) days of receipt. Disagreements under this clause will be resolved per Section 21 of the Agreement.

5. Acceptance of Deliverables

Upon completion of any deliverable set forth in a mutually executed SOW, AssetWorks shall provide a copy thereof to Customer. At such time, if Customer requests, AssetWorks will demonstrate to Customer that the deliverable conforms to the description specified for such deliverable in the SOW. If the deliverable does not conform to the description for such deliverable specified in a SOW, Customer shall have three (3) business days after AssetWorks' submission of the deliverable ("Acceptance Period") to give AssetWorks written notice which shall specify the deficiencies in detail. AssetWorks shall promptly cure any such deficiencies. After completing such cure, AssetWorks shall resubmit the deliverable for Customer review. Upon accepting any deliverable submitted by AssetWorks, Customer shall provide AssetWorks with written acceptance of such deliverable. If Customer fails to provide written notice of any deficiencies within the Acceptance Period, as provided above, such deliverable shall be deemed accepted at the end of the Acceptance Period.

SCHEDULE 5. FEE SCHEDULE.

SCHEDULE 6. DATA PROCESSING AGREEMENT.

This Data Processing Agreement ("**DPA**") is a legally enforceable contract entered into and made effective as of **[insert date]** ("**Effective Date**") by and between GoAssetWorks Limited ("**Service Provider**") and **[insert name]** ("**Customer**"). Service Provider and Customer are sometimes referred to in this DPA individually as a "**Party**" and collectively as the "**Parties**".

This DPA is incorporated by reference into the main agreement between the Parties for the provision by Service Provider to Customer of Service Provider's software and/or services (such software and/or services being the "Services" and such agreement being the "**Main Agreement**"). Notwithstanding its mutual execution, this DPA shall apply only to the extent Customer is established within the EEA (as defined below) or Switzerland or is otherwise caught by applicable EEA or Swiss data protection laws by virtue of their extra-territorial effect.

Definitions

In this DPA:

- Applicable Law** means as applicable and binding on the Customer, Service Provider and/or the Services:
- (a) any law, statute, regulation, by-law or subordinate legislation in force from time to time to which a Party is subject and/or in any jurisdiction that the Services are provided to or in respect of;
 - (b) the common law and laws of equity as applicable to the Parties from time to time;
 - (c) any binding court order, judgment or decree; or
 - (d) any applicable direction, policy, rule or order that is binding on a Party and that is made or given by any regulatory body having jurisdiction over a Party or any of that Party's assets, resources or business;

Business Days	a day other than a Saturday, Sunday or public holiday in in the country in which the Services are provided;
Data Controller	has the meaning given to that term (or to the term 'controller') in Data Protection Laws;
Data Processor	has the meaning given to that term (or to the term 'Processor') in Data Protection Laws;
Data Subject	has the meaning given to that term in Data Protection Laws;
Data Subject Request	means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;
Data Protection Laws	means as applicable and binding on the Customer, Service Provider and/or the Services: (a) in the United Kingdom: (i) the Data Protection Act 2018; and/or (ii) the GDPR, and/or any corresponding or equivalent national laws or regulations; (b) in member states of the European Union: the GDPR and all relevant member state laws or regulations giving effect to, replacing or supplementing the same; and (c) any Applicable Laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time;
Data Protection Losses	means all liabilities arising under Data Protection Laws, including all: (a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and (b) to the extent permitted by Applicable Law: (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (ii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and (iii) the reasonable costs of compliance with investigations by a Supervisory Authority;
EEA	means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein, as well as, for the purposes of this DPA, the United Kingdom.
GDPR	means the General Data Protection Regulation (EU) 2016/679;
International Recipient	has the meaning given to that term in Section 6.1;
Personal Data	has the meaning given to that term in Data Protection Laws;
Personal Data Breach	means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

Processing	has the meaning given to that term in Data Protection Laws (and related terms such as Process have corresponding meanings);
Processing Instructions	has the meaning given to that term in Section 2.1.1;
Protected Data	means Personal Data received from or on behalf of the Customer in connection with the performance of Service Provider 's obligations under this DPA or otherwise under the Main Agreement;
Standard Contractual Clauses	means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission in Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these;
Sub-Processor	means another Data Processor engaged by Service Provider for carrying out Processing activities in respect of the Protected Data on behalf of the Customer; and
Supervisory Authority	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.

References to any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting or consolidating such Applicable Law (including the GDPR and any new Data Protection Laws from time to time) and the equivalent terms defined in such Applicable Laws, once in force and applicable.

A reference to a law includes all subordinate legislation made under that law.

1 Data Processor and Data Controller

- 1.1** The Parties agree that, for the Protected Data, the Customer shall be the Data Controller and Service Provider shall be the Data Processor.
- 1.2** Service Provider shall Process Protected Data in compliance with:
 - 1.2.1** the obligations of Data Processors under Data Protection Laws in respect of the performance of its obligations under this DPA; and
 - 1.2.2** the terms of this DPA.
- 1.3** The Customer shall comply with:
 - 1.3.1** all Data Protection Laws in connection with the Processing of Protected Data, the Services and the exercise and performance of its respective rights and obligations under this DPA, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and
 - 1.3.2** the terms of this DPA.
- 1.4** The Customer warrants, represents and undertakes, that:
 - 1.4.1** all data sourced by the Customer for use in connection with the Services, prior to such data being provided to or accessed by Service Provider for the performance of the Services under this DPA, shall comply in all respects, including in terms of its collection, storage and Processing, with Data Protection Laws (which shall include the Customer providing all of the required fair Processing information to Data Subjects and maintaining for the term of this DPA the necessary legal grounds for transferring the Protected Data to Service Provider and allowing Service Provider to perform the Processing contemplated by this DPA);
 - 1.4.2** all instructions given by it to Service Provider in respect of Personal Data shall at all times be in accordance with Data Protection Laws;

- 1.4.3 it has undertaken due diligence in relation to Service Provider's Processing operations, and it is satisfied that:
- (a) Service Provider's Processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage Service Provider to Process the Protected Data; and
 - (b) Service Provider has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws;
- 1.4.4 it shall notify the Service Provider in the event of any change to the nature of the Protected Data, including its type and the categories of the relevant Data Subjects.
- 1.5 The Customer shall not withhold, delay or condition its agreement to any change requested by Service Provider in order to ensure the Services and Service Provider (and each Sub-Processor) can comply with Data Protection Laws.

2 Instructions and details of Processing

- 2.1 Insofar as Service Provider Processes Protected Data on behalf of the Customer, Service Provider:
- 2.1.1 unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) Process the Protected Data as agreed under the Main Agreement and in accordance with Service Provider's standard procedures, this DPA, and Schedule 1 hereto (together, the "**Processing Instructions**");
- 2.1.2 if Applicable Law requires it to Process Protected Data other than in accordance with the Processing Instructions, shall inform the Customer of any such requirement before Processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and
- 2.1.3 shall inform the Customer if Service Provider becomes aware of a Processing Instruction that, in Service Provider's opinion, infringes Data Protection Laws, provided that:
- (a) this shall be without prejudice to Sections 1.3 and 1.4; and
 - (b) to the maximum extent permitted by mandatory law, Service Provider shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any Processing in accordance with the Customer's additional Processing Instructions following the Customer's receipt of that information.

3 Technical and organisational measures

- 3.1 Service Provider shall implement and maintain, at its cost and expense, the technical and organisational measures set out in Schedule 2, provided that Service Provider reserves the right to make changes to such technical and organisational measures, 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 the Data Subjects.
- 3.2 Any additional technical and organisational measures are subject to agreement by Service Provider and shall be at the Customer's cost and expense.
- 3.3 The Customer shall ensure that, if feasible, any Protected Data in respect of which Service Provider is requested to provide support and maintenance services under this agreement are anonymised prior to Service Provider being granted access to them.

4 Using staff and other Processors

- 4.1 Customer agrees that Service Provider may engage Sub-Processors. Service Provider will impose on such Sub-Processors data protection terms that protect the Protected Data to the same standard provided for by this DPA. Upon Customer's request, Service Provider will provide to Customer a list of the then-current Sub-Processors.
- 4.2 Service Provider may, by giving no less than 30 days' prior notice to Customer, add or make changes to the Sub-Processors. Customer may object to the appointment of an additional Sub-Processor within 14 calendar days of such notice on reasonable grounds relating to the protection of the Protected Data, in which case

Service Provider shall have the right to cure the objection through one of the following options (to be selected at Service Provider's sole discretion):

- 4.2.1 Service Provider will cancel its plans to use the Sub-Processor with regard to Protected Data or will offer an alternative to provide the Services without such Sub-Processor; or
- 4.2.2 Service Provider will take the corrective steps requested by Customer in its objection (which remove Customer's objection) and proceed to use the Sub-Processor with regard to Protected Data; or
- 4.2.3 Service Provider may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the Services that would involve the use of such Sub-Processor with respect to Protected Data, subject to a mutual agreement of the Parties to adjust the remuneration for the Services.

If none of the above options are reasonably available and the objection has not been resolved to the mutual satisfaction of the Parties within 30 days after Service Provider's receipt of Customer's objection, either Party may terminate the Main Agreement for its convenience pursuant to the terms of the Main Agreement, or, if the Main Agreement contains no such terms, on no less than 60 days' advance written notice.

- 4.3 Service Provider may replace a Sub-Processor without advance notice to Customer if the reason for the change is beyond Service Provider's reasonable control, in which event Service Provider shall notify Customer of the replacement as soon as reasonably practicable and Customer shall retain the right to object to the replacement Sub-Processor pursuant to Section 4.2 above.
- 4.4 To the extent the appointment of any Sub-processor may result in the transfer of Protected Data outside the EEA to a country not recognised by the European Commission as having an adequate level of protection for Personal Data, Customer hereby authorizes Service Provider to enter into Standard Contractual Clauses with such Sub-processor as agent on its behalf to ensure the adequate protection of the transferred Personal Data, or such other arrangement as the Customer may approve as providing an adequate protection in respect of the processing of Protected Data in such third country.
- 4.5 Service Provider shall ensure that all Service Provider personnel authorised to Process Protected Data are subject to a binding written contractual obligation with Service Provider to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case Service Provider shall, where practicable and not prohibited by Applicable Law, notify the Customer of any such requirement before such disclosure) or are under an appropriate statutory obligation of confidentiality.

5 Assistance with the Customer's compliance and Data Subject rights

- 5.1 Service Provider shall provide commercially reasonable assistance, including by appropriate technical and organizational measures as reasonably practicable, to enable Customer to respond to any Data Subject Request, including rights of access, correction, restriction, objection, erasure, or data portability, as applicable. Service Provider shall refer all Data Subject Requests it receives to the Customer within 3 Business Days of receipt of the request, provided that for unreasonably complex or numerous requests (as determined by Service Provider in its sole and reasonable discretion) the Customer shall pay Service Provider's fees at Service Provider's rates from time to time in force for recording, referring, or otherwise dealing with the Data Subject Requests in accordance with this Section 5.1. For the avoidance of doubt, Customer is responsible for responding to Data Subject Requests.
- 5.2 Service Provider shall provide such reasonable assistance as the Customer reasonably requires (taking into account the nature of Processing and the information available to Service Provider) to the Customer in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to:
 - 5.2.1 security of Processing;
 - 5.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);
 - 5.2.3 prior consultation with a Supervisory Authority regarding high risk Processing; and
 - 5.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach,

provided the Customer shall pay Service Provider's generally applicable fees for providing the assistance in this Section 5.2, including time and materials rates or fees for additional technical measures such as software.

6 International data transfers

- 6.1** Subject to the terms of the Main Agreement, the Customer agrees that Service Provider may transfer Protected Data to countries outside the EEA or to any international organisation(s) (an “**International Recipient**”), provided all transfers by Service Provider of Protected Data to an International Recipient shall be effected in accordance with Data Protection Laws. In the event any such transfer results in Protected Data being transferred to a country which is not recognized by the European Commission as having an adequate level of protection for Personal Data, the Standard Contractual Clauses set out in Schedule 3 to this DPA shall apply.
- 6.2** The provisions of this DPA shall constitute the Customer’s instructions with respect to transfers in accordance with Section 2.1. Service Provider will provide a list of any such International Recipients upon request.

7 Records, information and audit

- 7.1** Service Provider shall maintain, in accordance with Data Protection Laws binding on Service Provider, written records of all categories of Processing activities carried out on behalf of the Customer.
- 7.2** Service Provider shall, in accordance with Data Protection Laws, make available to the Customer such information as is reasonably necessary to demonstrate Service Provider’s compliance with the obligations of Data Processors under Data Protection Laws.
- 7.3** Audits by Customer of Service Provider’s activities under this DPA will be as set out in the Main Agreement. If the Main Agreement does not include audit rights, Service Provider and Customer will discuss and agree in advance on the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit, and Service Provider reserves the right to charge a fee (based on Service Provider’s reasonable costs) for any such audit. Service Provider will provide further details of any applicable fee and the basis of its calculation to Customer in advance of any such audit. Any such audit shall be conducted in such a manner that the Service Provider’s undertakings toward third parties (including, but not limited to, the Service Provider’s customers, partners, and vendors) are in no way jeopardized. All Customer’s representatives or external auditors participating in any such audit shall execute customary confidentiality undertakings towards the Service Provider.

8 Breach notification

- 8.1** In respect of any Personal Data Breach involving Protected Data, Service Provider shall, without undue delay after becoming aware of the Personal Data Breach:
- 8.1.1 notify the Customer of the Personal Data Breach; and
 - 8.1.2 provide the Customer with details of the Personal Data Breach.

9 Term

- 9.1** This DPA shall commence on the Effective Date and shall terminate on the earlier of: (1) the termination of the Main Agreement; or (2) the mutual written agreement of the Parties.

10 Deletion or return of Protected Data and copies

- 10.1** Service Provider shall, at the Customer’s written request, either delete or return all the Protected Data to the Customer in such form as the Customer reasonably requests within a reasonable time after the earlier of:
- 10.1.1 the end of the provision of the relevant Services related to Processing; or
 - 10.1.2 once Processing by Service Provider of any Protected Data is no longer required for the purpose of Service Provider’s performance of its relevant obligations under this DPA, and delete existing copies,
- unless storage of any data is required by Applicable Law, in which case Service Provider shall inform the Customer of any such requirement.

11 Liability

- 11.1** The disclaimers and limitations of liability set out under the Main Agreement shall apply also to this DPA.

12 Survival of data protection provisions

- 12.1** Sections 1 to 13 (inclusive) shall survive termination (for any reason) or expiry of this DPA and continue:

12.1.1 indefinitely in the case of Sections 10 to 13 (inclusive); and

12.1.2 until 12 months following the earlier of the termination or expiry of this DPA in the case Sections 1 to 8 (inclusive), provided always that any termination or expiry of Sections 1 to 8 (inclusive) shall be without prejudice to any accrued rights or remedies of either party under any such Sections at the time of such termination or expiry.

13 Miscellaneous

- 13.1** In case of any conflict between this DPA and the Main Agreement, the provisions of this DPA shall control as regards the Processing of Protected Data unless expressly stated otherwise herein.

- 13.2** In the event the Standard Contractual Clauses apply pursuant to Section 6.1, in case of any conflict between the main body and Schedules 1 and 2 of this DPA and the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses shall control.

- 13.3** Any claims brought under or pursuant to this DPA or otherwise related hereto shall be subject to the terms and conditions of the Main Agreement, including, but not limited to, the exclusions to and limitations of liability set forth therein which shall apply to the liabilities and indemnities under and in connection with this DPA.

SCHEDULE 1 to DPA
PROCESSING INSTRUCTIONS

Instructions

The Customer hereby instructs the Service Provider to carry out Processing of the Customer's Personal Data for the performance of Services, as per the Main Agreement.

If the Service Provider entrusts the Processing of the Customer's Protected Data to Sub-Processors, the Service Provider is responsible for entering into written agreements with them. The Service Provider is responsible for ensuring that the Customer's instructions are sent to any Sub-Processors.

1.1 Purpose of the Processing

Processing of the Protected Data shall take place in accordance with the purpose in the Main Agreement.

1.2 General description of the Processing

[Insert detailed description of the types of Processing that Service Provider is to carry out, including the Processes, duration and nature of the Processing.]

[While some personal data can be stored within the application, personal data is not used for any transactional processing nor is the customer required to process any personal data; it is at the Customer's discretion to determine what personal data will be used and is typically determined during project implementation.]

1.3 Types of personal data

The Protected Data includes Personal Data of the categories checked off below.

Personal Data:

☒ Personal Data

Sensitive Personal Data:

- ☐ Racial or ethnic origin
- ☐ Political opinions
- ☐ Religious beliefs
- ☐ Philosophical beliefs
- ☐ Trade union membership
- ☐ Data concerning health including abuse of medicine, narcotics, alcohol etc.
- ☐ Data concerning sex life or sexual orientation

Data on purely private matters of individuals:

- ☐ Criminal offences
 - ☐ Significant social problems
 - ☐ Other purely private matters, which are not mentioned above:
-

1.4 Categories of data subjects

Data regarding the following categories of data subjects (for example, citizens, pupils, recipients of cash benefits, etc.) are Processed:

A) *Employees of the Organization*

C) *[Insert category of people]*

SCHEDULE 2 to DPA
TECHNICAL AND ORGANIZATIONAL MEASURES

Below, the Service Provider will positively indicate, e.g. ☒, or otherwise state, the applicable technical and organizational security measures within each section that have been applied to the Processing of Protected Data associated with this agreement.

1. Confidentiality (Article 32 (1)(a) and (b) GDPR)

Aim: To prevent unauthorized access or disclosure of protected data to individuals, entities or Processes.

- Physical Access Control - No unauthorised access to Data Processing Facilities, e.g.:
 - ✓ Use of magnetic or chip cards
 - ✓ Keys
 - ✓ Electronic door openers
 - ✓ Facility security services and/or entrance security staff
 - ✓ Alarm systems
 - ✓ Video/CCTV Systems
 - ☐ Other (Specify below)

- Electronic Access Control - No unauthorised use of the Data Processing and Data Storage Systems, e.g.:
 - ✓ Firewall,
 - ✓ Use of (secure) passwords
 - ✓ Automatic blocking/locking mechanisms
 - ✓ Two-factor authentication
 - ✓ Encryption of data carriers/storage media
 - ☐ Other (Specify below)

- Internal Access Control (permissions for user rights of access to and amendment of data) - No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g.:

- ✓ Rights authorisation concept
- ✓ Need-based rights of access / role-based access control
- ✓ Logging of system access events
- ☐ Other (Specify below)

- Isolation Control - The isolated Processing of data e.g.:
 - ✓ Multiple tenant/client support
 - ✓ Sandboxing
 - ☐ Other (Specify below)

- Pseudonymisation - The Processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.
 - ✓ Pseudonymisation
 - ☐ Anonymization
 - ☐ Scrambling
 - ☐ Masking
 - ☐ Blurring
 - ☐ Other (Specify below)

2. Integrity (Article 32 (1)(b) GDPR)

Aim: To provide assurance of consistency, accuracy and trustworthiness of protected data.

- Data Transfer Control - No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.:
 - ✓ Certificate based controls, (HTTPS, FTPS etc.)

- ✓ Use of encryption
- ✓ Virtual Private Networks (VPN)
- ✓ Electronic/digital signature
- ✓ Checksums
- ☐ Other (Specify below)

- Data Entry Control - Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.:
 - ✓ Use of Logging,
 - ✓ Document Management,
 - ✓ Quality control,
 - ✓ Change management
 - ☐ Other (Specify below)

- Data Integrity Control - Awareness or control of changes to data.: e.g.:
 - ✓ File integrity monitoring
 - ✓ Rights management
 - ✓ Value limit
 - ✓ Completeness
 - ✓ Validation
 - ✓ Entity
 - ☐ Other (Specify below)

3. Availability and Resilience (Article 32 (1)(b) GDPR)

Aim: To ensure that information is accessible to authorized individuals, entities, or Processes when needed.

- Availability Control, e.g.:
 - ✓ Backup Strategy (online/offline; on-site/off-site)

- ✓ Capacity plans
- ✓ Uninterruptible Power Supply (UPS)
- ✓ Virus protection
- ✓ Reporting procedures
- ✓ Contingency planning
- ☐ Other (Specify below)

- Ability for timely recovery (Article 32 (1)(c) GDPR); e.g.:
 - ✓ Use of backup strategy – recovery time objectives, recovery point objectives
 - ✓ Disaster recovery plans
 - ☐ Other (Specify below)

- Architectural Control; To reduce the possibility of loss of service through architectural/structural design e.g.:
 - ✓ High availability designs
 - ✓ Load balancing
 - ✓ Redundancy
 - ✓ Failover
 - ✓ Raid configurations
 - ✓ Software update/upgrade Processes
 - ✓ Patch management
 - ☐ Other (Specify below)

4. Effectiveness - Procedures for regular testing, assessment and evaluation (Article 32 (1)(d) GDPR)

- Data Protection Management, e.g.:
 - ✓ Use of data register
 - ✓ Data inventory
 - ✓ User awareness training
 - ☐ Other (Specify below)

- Data Privacy Impact Assessments, e.g.:
 - ✓ Continued use of Privacy Impact Assessments
 - ✓ General risk assessments
 - ☐ Other (Specify below)

- Incident Response Management; e.g.:
 - ✓ Use of the corporate Incident handling procedure
 - ✓ Use of industry standard security incident handling procedures
 - ☐ Other (Specify below)

- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR); e.g.:
 - ✓ Pseudonymisation
 - ✓ Data minimization
 - ✓ Data segregation
 - ✓ Role base access controls
 - ✓ Encryption at rest
 - ☐ Other (Specify below)

- Order or Contract Control - No third-party data Processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.:
 - ✓ Clear and unambiguous contractual arrangements
 - ✓ Formalised Order Management
 - ✓ Due diligence in selection of the Sub-Processor,

- ✓ Duty of pre-evaluation
- ✓ Duty of protection assurance
- ✓ Supervisory follow-up checks
- ☐ Other (Specify below)

SCHEDULE 3 to DPA
STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

The Customer is (the “data exporter”)

And

The Service Provider is (the “data importer”),

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) personal data, special categories of data, process/processing, controller, processor, data subject and supervisory authority shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) the data exporter means the controller who transfers the personal data;

(c) the data importer means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) the sub-processor means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract;

(e) the applicable data protection law means the legislation protecting the fundamental rights and freedoms of

individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) technical and organisational security measures means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause 3, Clause 4(b) to Clause 4(i), Clause 5(a) to Clause 5(e) and Clause 5(g) to Clause 5(j), Clause 6.1 and Clause 6.2, Clause 7, Clause 8.2 and Clause 9 to Clause 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to Clause 5(e) and Clause 5(g), Clause 6, Clause 7, Clause 8.2 and Clause 9 to Clause 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to Clause 5(e) and Clause 5(g), Clause 6, Clause 7, Clause 8.2, and Clause 9 to Clause 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2 and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to Clause 4(i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with Clause 11; and
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or its sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under

such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

IN WITNESS WHEREOF, the Clauses have been executed as of the date of the last party to sign below ("Effective Date"). If signed in counterparts, then each shall be considered an original thereof.

Customer:

Service Provider:

Signature

Signature

Name and Title

Name and Title

Date

Date

APPENDIX 1 – DETAILS OF PROCESSING

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix 1.

Data exporter

Customer (as defined in this Agreement)

Data importer

Service Provider (as defined in this Agreement).

Data subjects

As per the details set out in Schedule 1 of this Data Processing Agreement.

Categories of data

As per the details set out in Schedule 1 of this Data Processing Agreement.

Special categories of data (if appropriate)

As per the details set out in Schedule 1 of this Data Processing Agreement.

Processing operations

As per the details set out in Schedule 1 of this Data Processing Agreement.

IN WITNESS WHEREOF, this Appendix has been executed as of the date of the last party to sign below ("Effective Date"). If signed in counterparts, then each shall be considered an original thereof.

Customer:

Service Provider:

Signature

Signature

Name and Title

Name and Title

Date

Date

APPENDIX 2 – Technical and Organizational Security Measures

Description of the technical and organisational security measures implemented by the data importer in accordance with Clause 4(d) and Clause 5(c) (or documents/legislation attached):

As per the measures set out in Schedule 2 of this Data Processing Agreement.

IN WITNESS WHEREOF, this Appendix has been executed as of the date of the last party to sign below (“Effective Date”). If signed in counterparts, then each shall be considered an original thereof.

Customer:

Service Provider:

Signature

Signature

Name and Title

Name and Title

Date

Date