

Data Protection Addendum

This Data Protection Addendum ("Addendum") is entered this ____/____/ 2018.

Between:

1. **Esteiro Business Solutions Limited** (UK company registration number 04292582) which has its registered office at Ryehills Park, West Haddon, Northamptonshire, NN6 7BX ("**Supplier**"); and
2. _____ which has its registered office at _____ ("**Customer**").

Background

- A. The Supplier and the Customer entered into an agreement on or around 15 May 2018 under which the Supplier [permits the Customer to use its Gold Vision software, which may include use on a subscription basis, and provides services, including support services, in connection with that software] (the "**Agreement**").
- B. The Supplier and the Customer wish to amend the Agreement to address the requirements of applicable data protection laws in so far as they apply to Customer Personal Data (as defined below).
- C. In consideration of the mutual obligations set out in this Addendum, the parties hereby agree that the terms set out herein shall be added as an addendum to the Agreement. Save as expressly modified by the terms of this Addendum, the terms of the Agreement shall remain in full force and effect. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.
- D. Capitalised terms used in this Addendum shall have the meanings set forth in this Addendum and where not defined herein shall have the meaning given to them in the Agreement.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below:

- 1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Customer Personal Data in respect of which the Customer is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Customer Personal Data in respect of which the Customer is subject to any other Data Protection Laws;
- 1.1.2 "**Customer Personal Data**" means any Personal Data Processed by the Supplier on behalf of the Customer pursuant to or in connection with the Agreement;
- 1.1.3 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other relevant territory;
- 1.1.4 "**Data Protection Manager**" means a person properly authorised to deal with all data protection issues on behalf of the Customer, including day-to-day

compliance, management, service or receipt of any notices or communications, the provision of guidance and the handling and resolution of data protection issues;

- 1.1.5 "EEA" means the European Economic Area;
 - 1.1.6 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;
 - 1.1.7 "GDPR" means EU General Data Protection Regulation 2016/679, once in force;
 - 1.1.8 "ICO" means the UK Information Commissioner's Office;
 - 1.1.9 "Restricted Transfer" means:
 - 1.1.9.1 a transfer of Customer Personal Data from the Customer to the Supplier; or
 - 1.1.9.2 an onward transfer of Customer Personal Data from Supplier to a Subprocessor,in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses;
 - 1.1.10 "Security & Backup Policy" means the Supplier's security and backup policy, available at <https://www.gold-vision.com/terms-and-conditions/security-and-backup-policy> ;
 - 1.1.11 "Services" means the services and other activities to be supplied to or carried out by or on behalf of Supplier for the Customer pursuant to the Agreement;
 - 1.1.12 "Standard Contractual Clauses" means the standard controller-processor contractual clauses approved by the ICO from time to time; and
 - 1.1.13 "Subprocessor" means any person (including any third party, but excluding any employees of Supplier) appointed by or on behalf of Supplier to Process Personal Data on behalf of the Customer in connection with the Agreement.
- 1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.
- 1.3 The word "include" shall be construed to mean include without limitation, and similar terms shall be construed accordingly.

2. Application

- 2.1 This Addendum shall apply only to the extent that the Supplier's provision of the Services, and in particular its Processing of Personal Data, is subject to the Data Protection Laws – namely where the Customer is based in the EEA and/or to the extent that the Supplier processes Personal Data of Data Subjects located in the EEA on behalf of the Customer.

3. Processing of Customer Personal Data

3.1 Supplier shall:

- 3.1.1 comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and
- 3.1.2 not Process Customer Personal Data other than on the Customer's documented instructions unless Processing is required by Applicable Laws to which the Supplier is subject, in which case Supplier shall to the extent permitted by Applicable Laws inform the Customer of that legal requirement before the relevant Processing of that Personal Data.

3.2 The Customer:

3.2.1 instructs Supplier to:

3.2.1.1 Process Customer Personal Data; and

3.2.1.2 in particular, transfer Customer Personal Data to any country or territory specified in Annex 1,

as reasonably necessary for the provision of the Services and consistent with the Agreement;

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in clause 3.2.1;

3.2.3 shall appoint a Data Protection Manager, who shall act as the point of contact for all issues relating to data protection, and advise the Supplier of any changes to the Data Protection Manager;

3.2.4 accepts and agrees that (i) access to and use of Customer Personal Data by Customer employees, officers, agents, contractors, suppliers or anyone accessing Customer Personal Data via the Customer's account, including any such access or use outside the EEA, is the responsibility of the Customer, (ii) the said usage and access comprises Processing necessary for the Supplier's performance of its contractual obligations to the Customer and so comprises lawful Processing in accordance with Schedule 2, section 2 of the Data Protection Act 1998 and/or Article 6(1)(b) GDPR.

3.3 Annex 1 to this Addendum sets out certain information regarding the Supplier's Processing of the Customer Personal Data as required by article 28(3) of the GDPR. Customer may request reasonable amendments to Annex 1 by written notice to Supplier from time to time as Customer reasonably considers necessary to meet those requirements. Any such amendment shall be effective only upon the consent of the Supplier, not to be unreasonably withheld or delayed. Nothing in Annex 1 (including as amended pursuant to this clause 3.3) confers any right or imposes any obligation on any party to this Addendum.

4. Supplier Personnel

4.1 Supplier shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Customer Personal Data, ensuring in each case that access is limited to those individuals who need to know/access the relevant Customer

Personal Data, as reasonably necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Supplier, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

- 5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Supplier shall in relation to the Customer Personal Data implement appropriate technical and organizational measures designed to ensure a level of security appropriate to that risk, as described in the Supplier's Security & Backup Policy, which the Customer hereby accepts as satisfying the Supplier's obligations under this clause.
- 5.2 In assessing the appropriate level of security, Supplier shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. Subprocessing

- 6.1 Customer hereby authorises Supplier to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Agreement.
- 6.2 Supplier may continue to use those Subprocessors already engaged by Supplier as at the date of this Addendum, subject to Supplier in each case as soon as practicable meeting the obligations set out in section 6.4.
- 6.3 Supplier shall give Customer prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 14 days of receipt of that notice, Customer notifies Supplier in writing of any objections (on reasonable grounds) to the proposed appointment, the Supplier shall not appoint that proposed Subprocessor until reasonable steps have been taken to address the objections raised by any Customer and been provided with a reasonable written explanation of the steps taken.
- 6.4 With respect to each Subprocessor, Supplier shall:
 - 6.4.1 ensure that the arrangement between the Supplier and the Subprocessor is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this Addendum;
 - 6.4.2 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between the Supplier and the Subprocessor; and
 - 6.4.3 provide to Customer for review such copies of its agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Customer may request from time to time.

7. Data Subject Rights

- 7.1 Taking into account the nature of the Processing, Supplier shall assist Customer by implementing appropriate technical and organisational measures, insofar as this is possible,

for the fulfilment of the Customer's' obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Supplier shall:

7.2.1 promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

7.2.2 ensure that it does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Supplier is subject, in which case Supplier shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before it responds to the request.

8. Personal Data Breach

8.1 Supplier shall notify Customer without undue delay upon Supplier becoming aware of a Personal Data Breach affecting Customer Personal Data and provide Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

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

9. Data Protection Impact Assessment and Prior Consultation

Supplier shall provide reasonable practical or commercial assistance to the Customer in connection with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which are reasonably required of the Customer by the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to the Customer. For the avoidance of doubt, the Supplier shall have no responsibility with respect to the provision of legal, regulatory or compliance advice or guidance, in respect of which the Customer accepts full responsibility.

10. Deletion or return of Customer Personal Data

10.1 Subject to sections 10.2 and 10.3, the Supplier shall, within 30 days of the cessation of any Services involving the Processing of Customer Personal Data ("**Cessation Date**") delete and procure the deletion of all copies of the Customer Personal Data.

10.2 The Customer agrees and accepts that under the terms of the Agreement it is able to take a copy of the Customer Personal Data at any time during the provision of the Services, including at any time prior to the Cessation Date. If, having used all reasonable efforts to do so, the Customer is unable to take a copy of the Customer Personal Data by that means, the Supplier shall upon request return a complete copy of all Customer Personal Data to Customer in such format as is reasonably requested by Customer, provided that the request is raised no later than 14 days after the Cessation Date.

10.3 The Supplier may retain Customer Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Supplier shall ensure the confidentiality of all such Customer Personal Data and shall

ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

11. Audit rights

11.1 Subject always to sections 11.2 and 11.3 below, the Supplier shall (i) provide to the Customer such information and assistance as may be reasonably required by the Customer to demonstrate the Supplier's compliance with this Addendum, and (ii) allow audits by the Customer, or an auditor appointed by the Customer, in relation to the Processing of Customer Personal Data by the Supplier.

11.2 The information and audit rights of the Customer described in clause 11.1 shall arise only to the extent that the Agreement does not otherwise provide the Customer with information and audit rights meeting the relevant requirements of Data Protection Law.

11.3 The Customer shall give the Supplier reasonable prior notice of not less than 30 days of its wish to carry out an audit or inspection in accordance with this clause 11 and the parties will discuss and agree the timing, scope, duration and other aspects in advance of the audit or inspection, subject always to the following conditions:-

11.3.1 all personnel appointed by the Customer to carry out an audit or inspection ("**Personnel**") must provide suitable written undertakings to the Customer, including undertakings regarding confidentiality and compliance with the Customer's codes of practice and regulations, including any relating to security or health and safety;

11.3.2 all Personnel must produce evidence of their identity and authority;

11.3.3 the Customer will avoid causing any damage, injury or disruption to the Supplier's premises, equipment, personnel and business while its Personnel are on those premises in the course of such an audit or inspection;

11.3.4 all audits and inspections shall be carried out only during the Customer's normal business hours, unless justified on an emergency basis and provided that the Customer has given an acceptable explanation of the grounds for the need for access outside normal business hours;

11.3.5 no more than one audit or inspection may be carried out in any calendar year; and/or

11.3.6 that the extent of access permitted to Personnel will be only that strictly required to establish the Customer's compliance with this Addendum and under no circumstances will the Personnel be entitled to access any data, systems, equipment or premises which may cause the Customer to breach any obligations to any third party, including breach of any contractual or confidentiality obligations.

12. Customer Warranties & Liability

12.1 The Customer hereby warrants and represents that:-

12.1.1 it has complied, and will at all relevant times comply, fully with all Applicable Laws in respect of the Customer Personal Data;

- 12.1.2 the Customer has obtained and will at all relevant times maintain all rights, permissions, consents and authorisations to permit the Supplier to Process the Customer Personal Data in accordance with the terms of the Agreement and this Addendum; and
- 12.1.3 the Processing of the Customer Personal Data in accordance with the Agreement will not infringe third party rights, including the rights of any Data Subject.
- 12.2 The Supplier's performance hereunder is conditional upon the warranties and representations given in clause 12.1.
- 12.3 The Customer acknowledges that when acting as a data processor, the Supplier is reliant on the Customer for direction as to the extent the Supplier is entitled to use and process the Customer Personal Data in connection with the Services. Consequently, the Supplier shall be entitled to relief from liability in circumstances where a Data Subject makes a claim or complaint with regards to the Supplier's actions to the extent that such actions result from instructions received from the Customer or any breach of this Addendum by the Customer.
- 12.4 For the avoidance of doubt, all exclusions and limitations under the Agreement apply equally to this Addendum.

13. General Terms

- 13.1 The parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity. This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

Order of precedence

- 13.2 Nothing in this Addendum reduces Supplier's obligations under the Agreement in relation to the protection of Personal Data or permits Supplier to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement.
- 13.3 With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Severance

- 13.4 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect from the date first set out above.

Customer

Signature _____

Name _____

Title _____

Date Signed _____

Esteiro Business Solutions Limited

Signature _____

Name _____

Title _____

Date Signed _____

ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement and this Addendum.

The nature and purpose of the Processing of Customer Personal Data

1: Customer data held for contract performance
2: Contact data held who have an interest in your products and services
3: Contact data held to manage other business relationships
4:
5:

The types of Customer Personal Data to be Processed

Contact name and contact details (e.g. e-mail, phone number)

Contact name, address, phone number, e-mail address, social media link
--

The categories of Data Subject to whom the Customer Personal Data relates:

(e.g. Internal, External, Financial, Historical, Social)

1:	5:
2:	6:
3:	7:
4:	8:

The obligations and rights of Customer

The obligations and rights of Customer are set out in the Agreement and this Addendum.

The territories to which the Customer requests the transfer of Personal Data:

1: United Kingdom	5:
2: EEA	6:
3:	7:
4:	8: