DATA PROTECTION ADDENDUM
CONFIDENTIAL

The undersigned party agreeing to these terms ("Data Owner") has entered into an agreement (as amended from time to time, the "Agreement") with SupplyPro, Inc., a Delaware corporation ("SupplyPro") under which SupplyPro, (a) has agreed to provide hardware, software and/or services (collectively, "Services") to Data Owner and (b) may process certain personal data in the course of SupplyPro's performance of the Services on behalf of Data Owner ("User Data").

Further, the Agreement may provide Data Owner with the right to resell (possibly through multiple levels) all or part of the Services to certain permitted third parties. If and as applicable, and subject to Sections 3.1.2 and 3.1.3 of this Addendum, Data Owner enters into this Addendum as processor for the benefit of those further permitted third parties who act as controllers (each, a "Third Party Controller") in respect of personal data processed by SupplyPro in performance of the Services on those further permitted third parties' behalf ("Third Party User Data").

This Data Protection Addendum, including its appendices (the "Addendum"), will be effective as of the Addendum Effective Date (as defined below) and shall apply to the processing of Personal Data (as defined below) solely to the extent that European Data Protection Legislation applies to such processing.

This Addendum supplements and forms part of the Agreement.

1. Definitions

For purposes of this Addendum, the terms below shall have the meanings set forth below. Capitalized terms that are used but not otherwise defined in this Addendum or the recitals above shall have the meanings set forth in the Agreement.

1.1 "Addendum Effective Date" means the date on which the parties agreed to this Addendum.

1.2 "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

1.3 "Compliance Documentation" has the meaning given in Section 5.4.4.

1.4 "EEA" means the European Economic Area.

1.5 "EU" means the European Union.

1.6 "EU GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

1.7 "EU Restricted Transfer" means a transfer of Personal Data to any person, which would be prohibited without a legal basis therefor under Chapter V of the EU GDPR.

1.8 "European Data Protection Legislation" means the GDPR and other data protection laws of the EU, its Member States, Switzerland, Iceland, Liechtenstein, Norway and the United Kingdom, in each case, applicable to the processing of Personal Data under the Agreement.

1.9 "GDPR" means the UK GDPR and/or EU GDPR (as applicable), together with any applicable implementing or supplementary legislation in any member state of the EEA or the UK (including the UK Data Protection Act 2018). References to "Articles" and "Chapters" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

1.10 "Information Security Incident" means a breach of SupplyPro's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data in SupplyPro's possession, custody or control. "Information Security Incidents" do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

1.11 "Personal Data" means any personal data contained within the User Data and Third Party User Data, which SupplyPro processes as a processor on behalf of Data Owner and/or any Third Party Controllers (as applicable).

1.12 "Restricted Country" (i) in the context of the UK, means a country or territory outside the UK; and (ii) in the context of the EEA, means a country or territory outside the EEA, that has not been deemed to provide an 'adequate' level of protection for Personal Data pursuant to a decision made in accordance with Article 45(1) of the GDPR.

1.13 "Restricted Transfer" means an EU Restricted Transfer and/or a UK Restricted Transfer, as the context requires.

1.14 "Security Documentation" means the Security Measures and any other documents and information made available by SupplyPro under Section 5.4 (Reviews and Audits of Compliance).

1.15 "Security Measures" has the meaning given in Section 5.1.1 (SupplyPro's Security Measures).

1.16 "Standard Contractual Clauses" means the standard contractual clauses issued and approved by the European Commission pursuant to implementing Decision (EU) 2021/914, a populated copy of which is attached hereto as Annex 4.

1.17 "Subprocessors" means third parties authorised under this Addendum to process Personal Data in relation to the Services.

1.18 "Supervisory Authority" (i) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office; and (ii) in the context of the EEA and EU GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR.

1.19 "Term" means the period from the Addendum Effective Date until the end of SupplyPro's provision of the Services.

1.20 "UK GDPR" means the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019).

1.21 "UK Restricted Transfer" means a transfer of Personal Data to any person, which would be prohibited without a legal basis therefor under Chapter V of the UK GDPR.

1.22 "UK Transfer Addendum" means the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the UK Mandatory Clauses included in Part 2 thereof (the "UK Mandatory Clauses").

1.23 The terms "data subject", "personal data", "processing", "controller", and "processor" as used in this Addendum have the meanings given in the GDPR.

2. Duration of Addendum

This Addendum will take effect on the Addendum Effective Date and, notwithstanding the expiration of the Term and/or expiration and/or termination of the Agreement, will remain in effect until, and automatically expire upon, SupplyPro's deletion of all Personal Data.

3. Processing of Data

3.1 Roles and Regulatory Compliance; Authorization.

3.1.1 Processor and Controller Responsibilities. The parties acknowledge and agree that:

(a) the subject matter and details of the processing are described in Annex 1;

(b) as between the parties:

(i) Data Owner acts the controller of Personal Data processed by SupplyPro in performance of the Services (including as may be resold to Third Party Controllers) under European Data Protection Legislation – however, it is noted that vis-à-vis Third Party Controllers, Data Owner acts as a processor on behalf of such Third Party Controllers; and

(ii) SupplyPro acts as a processor of Personal Data it processes in performance of the Services – however, it is noted that vis-à-vis Third Party Controllers, SupplyPro acts as a sub-processor on behalf of such Third Party Controllers who themselves act through Data Owner (being, as noted in (i) above, a processor vis-à-vis Third Party Controllers in such context); and

(c) each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Personal Data.

3.1.2 Third Party Controllers. If and to the extent that:

(a) Data Owner acts as a processor on behalf of a Third Party Controller; or

(b) Data Owner otherwise causes SupplyPro to process any Personal Data on behalf of a Third Party Controller,

Data Owner represents and warrants to SupplyPro that:

(y) Data Owner's instructions and actions with respect to Personal Data processed on the relevant Third Party Controller's behalf (including its appointment of SupplyPro as another processor and the appointment of Subprocessors in accordance with Section 9); and

(z) SupplyPro's processing of any Personal Data on behalf of such Third Party Controller in performance of the Services (including as any part thereof may have been resold to such Third Party Controller), have been fully and effectively authorized by that Third Party Controller.

3.1.3 Third Party Controllers (cont'd.). The parties acknowledge and agree that insofar as SupplyPro processes Personal Data on behalf of a Third Party Controller, in the other Sections of this Addendum, where the context permits and requires, the term 'Data Owner' shall be construed to refer to that Third Party Controller to the extent required to enable Third Party Controllers to comply with applicable European Data Protection Legislation concerning appointment of Processors, **PROVIDED THAT** it is acknowledged and agreed that:

(a) Third Party Controllers shall have no right or entitlement to exercise or seek any rights or remedies under this Addendum;

(b) any rights and any remedies under this Addendum shall accrue, and may only be exercised and sought by Data Owner, on a collective and not an individual basis, on behalf of Data Owner and all Third Party Controllers – *for example*: (i) any on-premise inspections that may occur in accordance with Section 5.4 shall be conducted for the benefit of Data Owner and all Third Party Controllers collectively, and the limits on the frequency of such audits shall apply on a collective basis; and (ii) any relevant notices (such as that referred to in Section 9.4 concerning new Subprocessors)

shall be given by SupplyPro to Data Owner only, and Data Owner (and not SupplyPro) shall be responsible for disseminating such notices to Third Party Controllers; and (iii) any right to object to new Subprocessors shall be exercisable only by Data Owner (and not a Third Party Controller); and

(c) SupplyPro shall have no liability whatsoever (whether in contract, tort (including for negligence), breach of statutory duty (howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise) arising out of or in connection with this Addendum to Third Party Controllers.

3.1.4 Data Owner Responsibilities. Data Owner represents and warrants that:

(a) Data Owner has established or ensured that another party (including, where applicable, the Third Party Controller) has established a legal basis for SupplyPro's processing of Personal Data contemplated by this Addendum;

(b) all notices have been given to, and obtained consents and rights have been obtained from, the data subjects to whom Personal Data relates and any other party as may be required under applicable law (including European Data Protection Legislation) for such processing;

(c) neither User Data nor Third Party User Data contains, nor will it contain, any special categories of personal data as described in Article 9(1) of GDPR, nor any personal data relating to criminal convictions and/or offences; and

(d) as at the Addendum Effective Date, it is not aware of any act, omission, event or circumstance that does or might constitute or give rise to a breach by either party (or, where applicable, any Third Party Controller) of any term of this Addendum.

3.2 Scope of Processing.

3.2.1 Data Owner's Instructions. By entering into this Addendum, Data Owner instructs SupplyPro to process Personal Data (a) to provide the Services (including as any part thereof may have been resold to such Third Party Controller); (b) as authorised by the Agreement, including this Addendum; and (c) as further documented in any other written instructions given by Data Owner and acknowledged in writing by SupplyPro as constituting instructions for purposes of this Addendum.

3.2.2 SupplyPro's Compliance with Instructions. SupplyPro will only process Personal Data in accordance with Data Owner's instructions described in Section 3.2.1.

4. Data Deletion

Deletion on cessation of Services. Upon the end of the provision of Services relating to any relevant processing of Personal Data carried out hereunder, SupplyPro shall (at the choice of Data Owner) either:

4.1.1 enable Data Owner or the relevant Third Party Controller (as directed by Data Owner) to use functionality within SupplyPro's cloud based software SupplySystem Intelligent Software to, within 30 days following the end of the provision of such Services, download a complete copy of all relevant Personal Data (using the following path: Log into SSIS at https://supplysystem.supplypro.com/ClientSite/Home > select 'Partners' or 'Clients' (as applicable) in the drop-down > select the Data Owner or relevant Third Party Controller's organisation > select 'Analytics' > select 'Reports' > expand 'User Reports' > select 'User Listing Details' > select appropriate parameters and then use the 'Schedule Report' or 'Send Now' function), and as soon as reasonably practicable thereafter to delete existing copies unless and to the extent European Union or Member State law requires otherwise; or

4.1.2 as soon as reasonably practicable thereafter delete all Personal Data, unless and to the extent local laws applicable to SupplyPro require otherwise.

5. Data Security

5.1 SupplyPro's Security Measures, Controls and Assistance.

5.1.1 SupplyPro's Security Measures. SupplyPro will implement and maintain technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data as described in Annex 2 (the "Security Measures").

5.1.2 Security Compliance by SupplyPro Staff. SupplyPro will grant access to Personal Data only to employees, contractors and Subprocessors who need such access for the scope of their performance,and are subject to appropriate confidentiality arrangements.

5.1.3 SupplyPro's Security Assistance. SupplyPro will (taking into account the nature of the processing of Personal Data and the information available to SupplyPro) provide Data Owner with reasonable assistance necessary for Data Owner to comply with its obligations in respect of Personal Data under European Data Protection Legislation, including Articles 32 to 34 (inclusive) of the GDPR, by:

(a) implementing and maintaining the Security Measures in accordance with Section 5.1.1 (SupplyPro's Security Measures);

(b) complying with the terms of Section 5.2 (Information Security Incidents); and

(c) providing Data Owner with the Security Documentation in accordance with Section 5.4.

5.2 Information Security Incidents

5.2.1 Information Security Incident Notification. If SupplyPro becomes aware of an Information Security Incident, SupplyPro will: (a) notify Data Owner of the Information Security Incident without undue delay after becoming aware of the Information Security Incident; and (b) take reasonable steps to identify the cause of such Information Security Incident, minimise harm and prevent a recurrence.

5.2.2 Details of Information Security Incident. Notifications made pursuant to this Section 5.2 (Information Security Incidents) will describe, to the extent possible, details of the Information Security Incident and steps SupplyPro recommends Data Owner take to address the Information Security Incident.

5.2.3 No Acknowledgement of Fault by SupplyPro. SupplyPro's notification of or response to an Information Security Incident under this Section 5.2 (Information Security Incidents) will not be construed as an acknowledgement by SupplyPro of any fault or liability with respect to the Information Security Incident, nor shall such notification or response relieve Data Owner and/or any Third Party Controller of its obligations to SupplyPro (including, where applicable, to pay sums when due and payable under and in accordance with the Agreement).

5.2.4 Relief. SupplyPro will not have any responsibility or liability whatsoever to the Data Owner and/or any Third Party Controller arising from or in relation to any Information Security Incident or any breach of this Section 5, to the extent caused or contributed to (directly or indirectly) by the Data Owner's or any applicable Third Party Controller's(s'), or any person acting on its or their behalf's:

(a) deployment, installation or other use of all or any part of the Services that is not permitted under and in accordance with the Agreement (including installation in a territory or jurisdiction not supported under the Agreement);

(b) combination, operation, linking, integration or other use of all or any part of the Services with products, services, data extractors, intellectual property, information, materials, technologies, methods or processes not furnished by or on behalf of SupplyPro or permitted under and in accordance with the Agreement;

(c) changes or modifications (including any changes to the system, software or firmware) to all or any part of the Services, which are not made, or authorized in writing, by SupplyPro;

(d) failure to install any system, software, or firmware update in any hardware or software owned or operated by Data Owner and/or Third Party Controller; and/or

(e) failure to install any Update within the timeframe recommended by SupplyPro or, in the absence of such recommended timeframe, a reasonable time after the Update is made generally available by SupplyPro, if such Information Security Incident or breach could have been avoided by the installation of such Update.

5.2.5 Additional Definitions. For the purposes of Section 5.2.4(e), "Update" means: (a) a patch release of any element of the relevant software which corrects faults (including security-related faults), adds functionality or otherwise amends any element of the relevant software; (b) a upgrade/update to the relevant software, which incorporates revisions, improvements and / or enhancements to the content, functionality, features, performance, security, quality and/or stability of the relevant software (including corrections and/or bug fixes); and /or (c) a new release of the relevant software that from time-to-time is publicly marketed and offered for purchase by SupplyPro, which is designed to run on a later version of the applicable operating system (e.g., an upgrade from Windows XP to Windows 8)

5.3 Data Owner's Security Responsibilities and Assessment.

5.3.1 Data Owner's Security Responsibilities. Data Owner agrees that, without limitation of SupplyPro's obligations under Section 5.1 (SupplyPro's Security Measures, Controls and Assistance) and Section 5.2 (Information Security Incidents):

(a) Data Owner is solely responsible for its use of the Services, including:

(i) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data;

(ii) securing the account authentication credentials, systems and devices Data Owner uses to access the Services;

(iii) securing Data Owner's systems and devices that SupplyPro uses to provide the Services; and

(iv) backing up its Personal Data; and

(b) SupplyPro has no obligation to protect Personal Data that Data Owner elects to store or transfer outside of SupplyPro's and its Subprocessors' systems.

5.3.2 Data Owner's Security Assessment.

(a) Data Owner is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures and SupplyPro's commitments under this Section 5 (Data Security) will meet Data Owner's needs, including with respect to any security obligations of Data Owner under the European Data Protection Legislation.

(b) Data Owner acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by SupplyPro as set out in Section 5.1.1 (SupplyPro's Security Measures) provide a level of security appropriate to the risk in respect of the Personal Data.

5.4 Reviews and Audits of Compliance

5.4.1 Data Owner may audit SupplyPro's compliance with its obligations under this Addendum up to once per year (which may include, subject to the remainder of this Section 5.4, on-site inspection of SupplyPro's environment in which Personal Data is processed by SupplyPro). In addition, to the extent required by European Data Protection Legislation, including where mandated by any supervisory authority having jurisdiction, Data Owner may perform more frequent audits (including inspections). SupplyPro will contribute to such audits by providing Data Owner or any supervisory authority having jurisdiction with the information and assistance reasonably necessary to conduct the audit, including any relevant records of processing activities applicable to the Services.

5.4.2 If a third party is to conduct the audit, SupplyPro may object to the auditor if the auditor is, in SupplyPro's reasonable opinion, not suitably qualified or independent, a competitor of SupplyPro, or otherwise manifestly unsuitable. Such objection by SupplyPro will require Data Owner to appoint another auditor or conduct the audit itself.

5.4.3 To request an audit, Data Owner must submit a detailed proposed audit plan to SupplyPro at least thirty (30) days in advance of the proposed audit date and sign a customary nondisclosure agreement mutually acceptable to the parties (which shall not be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. SupplyPro will review the proposed audit plan and provide Data Owner with any concerns or questions (for example, any request for information that could compromise SupplyPro security, privacy, employment or other relevant policies). SupplyPro will work cooperatively with Data Owner to agree on a final audit plan. Nothing in this Section 5.4 shall require SupplyPro to breach any duties of confidentiality.

5.4.4 If the controls or measures to be assessed in the requested audit are addressed in any of the following, Data Owner agrees to accept it in lieu of requesting an audit of such controls or measures: (a) an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of Data Owner's audit request and SupplyPro has confirmed there are no known material changes in the controls audited; (b) an approved code of conduct described in Article 40 of the GDPR to which SupplyPro adheres; or (c) an approved certification mechanism described in Article 42 of the GDPR under which SupplyPro is certified ("Compliance Documentation").

5.4.5 The audit must be conducted during regular business hours, subject to the agreed final audit plan and SupplyPro's health and safety or other relevant policies, and may not unreasonably interfere with SupplyPro business activities.

5.4.6 Data Owner will promptly notify SupplyPro of any non-compliance discovered during the course of an audit and provide SupplyPro any audit reports generated in connection with any audit under this Section 5.4, unless prohibited by European Data Protection Legislation or otherwise instructed by a supervisory authority. Data Owner may use the audit reports only for the purposes of meeting Data Owner's regulatory audit requirements and/or confirming compliance with the requirements of this Addendum.

5.4.7 Any audits are at Data Owner's expense. Data Owner shall reimburse SupplyPro for any time expended by SupplyPro or its Subprocessors in connection with any audits or inspections under this Section 5.4 at SupplyPro's then-current professional services rates, which shall be made available to Data Owner upon request. Data Owner will be responsible for any fees charged by any auditor appointed by Data Owner to execute any such audit. Nothing in this Addendum shall be construed to require SupplyPro to furnish more information about its Subprocessors in a connection with such audits than such Subprocessors make generally available to their customers.

6. Impact Assessments and Consultations

SupplyPro will take reasonable steps to assist Data Owner in complying with the Data Owner's obligations under European Data Protection Legislation to: (a) perform data protection impact assessments if and to the extent SupplyPro's processing of Personal Data is likely to result in a high risk to the rights and freedoms of affected data subjects; and (b) consult with a relevant supervisory authority if and to the extent any such data protection impact assessment determines (having been performed in good faith) that SupplyPro's processing of Personal Data would result in a high risk to affected data subjects in the absence of measures taken to by Data Owner and/or SupplyPro in mitigation thereof. Data Owner's rights, and SupplyPro's obligations, under this Section 6 shall only arise if and to the limited extent that Data Owner is expressly obliged to take the steps described herein (taking into account the nature of the processing and the information available to SupplyPro, and relevant limitations set out in Articles 35 and 36 of the GDPR) under European Data Protection Legislation. SupplyPro reserves the right to charge the Data Owner for, and in such event the Data Owner shall pay to SupplyPro, any costs incurred in the provision of assistance under this Section 6 at SupplyPro's then-current professional services rates.

7. Data Subject Rights

7.1 Data Owner's Responsibility for Requests. During the Term, if SupplyPro receives any request from a data subject in relation to Personal Data, SupplyPro will (i) notify the Data Owner; and (ii) advise the data subject to submit their request to Data Owner and Data Owner will be responsible for responding to any such request. Data Owner acknowledges and agrees that, (a) for the purposes of Clause 15.1(a) of the Standard Contractual Clauses, except to the extent prohibited by applicable law and/or the relevant public authority, as between the parties, Data Owner acknowledges and agree that it shall be solely responsible for making any notifications to relevant data subjects if and as required; and (b) for the purposes of Clause 10(a) of Module Three of the Standard Contractual Clauses, there are no circumstances in which it would be appropriate for SupplyPro to notify any Third Party Controller of any data subject request and that any such notification shall be the responsibility of Data Owner.

7.2 SupplyPro's Data Subject Request Assistance. SupplyPro will (taking into account the nature of the processing of Personal Data) provide Data Owner with self-service functionality through the Services or other reasonable assistance as necessary for Data Owner to fulfil its obligation under European Data Protection Legislation to respond to requests by data subjects, including if applicable, Data Owner's obligation to respond to requests for exercising the data subject's rights set out in Chapter III of the GDPR. Data Owner shall reimburse SupplyPro for any such assistance beyond providing self-service features included as part of the Services at SupplyPro's then-current professional services rates, which shall be made available to Data Owner upon request.

8. Data Transfers

8.1 Data Storage and Processing Facilities. SupplyPro may, subject to Sections 8.2 and 8.3, store and process Personal Data in the United States or anywhere SupplyPro or its Subprocessors operate.

8.2 Standard Contractual Clauses. In relation to any Restricted Transfer associated with the processing by SupplyPro in the United States, the Parties shall comply with their respective obligations set out in the Standard Contractual Clauses, which are deemed to be entered into with effect from the first date of any such: (a) EU Restricted Transfer; and/or (b) any UK Restricted Transfer (as populated and varied in the manner set out in Section 8.3). Furthermore, the Parties acknowledge and agree that:

8.2.1 the provisions of Module 2 of the Standard Contractual Clauses shall apply in respect of any such Restricted Transfer(s) associated with the processing of Personal Data in respect of which Data Owner is a controller; and

8.2.2 the provisions of Module 3 of the Standard Contractual Clauses shall apply in respect of any such Restricted Transfer(s) associated with the processing of Personal Data in respect of which Data Owner is a processor (including where it acts on behalf of a Third Party Controller), in each case as described in Section 3.1 above.

8.3 UK Transfer Addendum. In relation to any UK Restricted Transfer associated with the processing by SupplyPro in the United States, the Standard Contractual Clauses entered into pursuant to Section 8.2 shall apply as varied by the UK Transfer Addendum in the following manner: (i) for the purposes of 'Part 1 to the UK Transfer Addendum': (A) the Parties agree: Tables 1, 2 and 3 to the UK Transfer Addendum are deemed populated with the corresponding details set out in Annex 1 (Subject Matter and Details of the Data Processing) and this Section 8.3, applying the Module(s) determined by Section 8.2; and (B) Table 4 to the UK Transfer Addendum is completed with 'Data Importer' only; and (ii) for the purposes of 'Part 2 to the UK Transfer Addendum': the Parties agree to be bound by the UK Mandatory Clauses of the UK Transfer Addendum and agree that the Standard Contractual Clauses shall apply to any UK Restricted Transfers as varied in accordance with those Mandatory Clauses. As permitted by section 17 of the UK Mandatory Clauses, the Parties agree to the presentation of the information required by 'Part 1: Tables' of the UK Transfer Addendum in the manner determined by this Section 8.3; provided that nothing in the manner of that presentation shall operate or be construed so as to reduce the Appropriate Safeguards (as defined in the UK Mandatory Clauses).

8.4 Order of Precedence. In the event of any conflict or inconsistency between any provision in this Addendum and any provision in the Standard Contractual Clauses, the relevant provision in the Standard Contractual Clauses shall prevail and govern in preference to the relevant provision in this Addendum to the extent of such conflict or inconsistency; provided that, it is agreed that the following shall apply:

8.4.1 when complying with its transparency obligations under Clause 8.3 of the Standard Contractual Clauses, Data Owner acknowledges and agrees that it shall not provide or otherwise make available, and shall take all appropriate steps to protect, SupplyPro and its licensors' trade secrets, business secrets, confidential information and/or other commercially sensitive information;

8.4.2 the audits described in Clauses 8.9(c) and 8.9(d) of the Standard Contractual Clauses shall be performed in accordance with Section 5.4 of this Addendum (Reviews and Audits of Compliance);

8.4.3 the authorization in Section 9 of this Addendum (Subprocessors) will constitute Data Owner's and any relevant Third Party Controller's (i) prior written consent to the subcontracting by SupplyPro of the processing of Personal Data for the purposes of Clause 9(a) of the Standard Contractual Clauses, in respect of which the Parties are deemed to have selected Option 2; and (ii) documented instructions to effect disclosures and onward transfers to any relevant Subprocessors if and as required under Clause 8 of the Standard Contractual Clauses and

8.4.4 certification of deletion of Personal Data as described in Clauses 8.5 and 16(d), of the Standard Contractual Clauses shall be provided only upon Data Owner's request (including any request made on behalf of any relevant Third Party Controller).

8.5 Notwithstanding the foregoing, the Standard Contractual Clauses will not apply to the extent an alternative recognized compliance standard under Chapter V of the GDPR for the lawful transfer of Personal Data to a Restricted Country applies to the relevant Restricted Transfer.

8.6 To the extent that Users who have access to Personal Data stored in the SupplyPro Services include individuals based in a Restricted Country:

8.6.1 Data Owner acknowledges and agrees that it is responsible for putting in place (or procuring that any applicable Third Party Controller shall put in place), and shall ensure that there are, appropriate legal bases and effective mechanisms to legitimise the transfer of such Personal Data to such individuals in the Restricted Country through (or in relation to) the use by such Users of the SupplyPro Services; and

8.6.2 Data Owner hereby instructs SupplyPro to enable such transfers, as anticipated by the programming of the settings of the SupplyPro Services agreed to by Data Owner.

9. Subprocessors

9.1 Requirements for Subprocessor Engagement. When engaging any Subprocessor, SupplyPro will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this Addendum with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. SupplyPro shall be liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

9.2 Information about Subprocessors. Information about Subprocessors, including their functions and locations, is set out in Annex 3 hereto (as may be updated from time to time in accordance with this Section 9) (the "Subprocessor List").

9.3 General Authorization to Subprocessor Engagement.

Data Owner hereby provides its general authorization to the engagement by SupplyPro of Subprocessors from time to time. SupplyPro may continue to use those Subprocessors already engaged by SupplyPro as at the date of this Addendum (as shown in the Subprocessor List). SupplyPro shall notify Data Owner of any addition or replacement of any Subprocessors at least fourteen (14) days prior to any such proposed addition or replacement.

9.4 Notification of Changes to Subprocessors. Data Owner acknowledges and agrees that the notification to be provided by SupplyPro pursuant to Section 9.3 may be so provided by way of a 'pop-up' banner notification displayed at the point of user log-in to the Software which shall appear at any such log-in occurring in the fourteen (14) day period prior to the proposed date of engagement of any such Subprocessor by SupplyPro (which Data Owner hereby accepts as good and sufficient notice for the purposes hereof (including Clause 9 of the Standard Contractual Clauses) and European Data Protection Legislation).

9.5 Opportunity to Object to Subprocessor Changes. If within ten (10) days of receipt of the notice pursuant to Section 9.4, Data Owner notifies SupplyPro in writing of any objections to the proposed appointment of any new Subprocessor on reasonable grounds (e.g., if a proposed Subprocessor's processing of Personal Data would cause Data Owner or a Third Party Controller to violate European Data Protection Legislation), SupplyPro shall either:

9.5.1 recommend a commercially reasonable change to Data Owner or the relevant Third Party Controller's configuration or use of the Services to avoid processing of Personal Data by the proposed Subprocessor in respect of whom an objection or withholding of authorization is made; and/or

9.5.2 use reasonable efforts to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor (as applicable).

9.6 Termination Rights. Where no changes referenced in Sections 9.5.1 or 9.5.2 can be made within the thirty (30) day period following SupplyPro's receipt of Data Owner's notice of objections (the "Change Period"), either Party may by written notice to the other, to be served within fourteen (14) days of the expiration of that Change Period, terminate the Agreement (either in whole or to the extent that it relates to the portion of the Services which requires the use of the proposed Subprocessor (as applicable)) with immediate effect.

9.7 Deemed authorization. If Data Owner and/or any Third Party Controller, uses the Services or the relevant portion thereof after the expiry of the fourteen (14) day period referred to in Section 9.6, Data Owner agrees that it shall be deemed to have authorized the ongoing use of that Subprocessor (as applicable) on its own behalf and behalf of each Third Party Controller.

10. Notices

Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by SupplyPro to Data Owner may be given (a) in accordance with the notice clause of the Agreement; (b) to SupplyPro's primary points of contact with Data Owner; and/or (c) to any email provided by Data Owner for the purpose of providing it with Service-related communications or alerts. Data Owner is solely responsible for ensuring that such email addresses are valid.

11. DMCA and WIPO Treaty Support

It is noted, for informational purposes only, that SupplyPro supports the Digital Millennium Copyright Act of 1998 and the World Intellectual Property Organization Copyright Treaty.

12. No denigration

Neither party shall make any statement (orally or in writing; publicly or privately) or do any act or otherwise engage in any activity that will or may disparage, denigrate or be detrimental to the other party and/or its Affiliates, and/or its or their business or affairs, and shall not authorise, permit or instruct any third party to do the same.

13. Liability

The total aggregate liability of each party towards the other party, howsoever arising, under or in connection with this Addendum and the Standard Contractual Clauses (if and as they apply) will under no circumstances exceed any limitations or caps on, and shall be subject to any exclusions of, liability and loss agreed by the parties in the Agreement (which, for the avoidance of doubt shall survive any expiration or termination of the Agreement); provided that, nothing in this Section 13 will affect any person's liability to data subjects under the third-party beneficiary provisions of the Standard Contractual Clauses (if and as they apply).

14. Effect of These Terms

Except as expressly modified by the Addendum, the terms of the Agreement remain in full force and effect. To the extent of any conflict or inconsistency between this Addendum and the remaining terms of the Agreement, this Addendum will govern.

Accepted and agreed to by the authorized representative of each party:

DATA OWNER **Company:**	**SUPPLYPRO, INC.**
Signature: _____	Signature: [signature]
Name:	Name: Doug Gilger
Title:	Title: VP Finance + Acct
Date:	Date: November 16, 2023

Annex 1

Subject Matter and Details of the Data Processing

Subject Matter	SupplyPro's provision of the Services to Data Owner or a Third Party Controller under and in accordance with the Agreement.
Duration of the Processing	The Term plus the period from the expiry of the Term until deletion of all Personal Data by SupplyPro in accordance with the Agreement and Section 4 of this Addendum.
Nature and Purpose of the Processing	SupplyPro will process Personal Data for the purposes of providing the Services to Data Owner or a Third Party Controller in accordance with the Agreement.
Categories of Data	In the context of Services provided for the benefit of Data Owner (in respect of which Data Owner itself acts as Controller): • Name • User name • Email address • Other contact details (e.g., business address, telephone number etc) • Any other Personal Data submitted to the Services In the context of Services provided for the benefit of Third Party Controllers (in respect of which Data Owner acts as Processor on behalf of such Third Party Controller): • Name • User name • Email address • Other contact details (e.g., business address, telephone number etc) • Any other Personal Data submitted to the Services
Data Subjects	In the context of Services provided for the benefit of Data Owner (in respect of which Data Owner itself acts as Controller): • Data Owner's employees, contractors, consultants, agents and other staff who use the Services under and in accordance with the Agreement ("Users") • Any other data subject(s) whose Personal Data is submitted to the Services by or on behalf of Data Owner's staff. In the context of Services provided for the benefit of Third Party Controllers (in respect of which Data Owner acts as Processor on behalf of such Third Party Controller): • Third Party Controllers' employees, contractors, consultants, agents and other staff who use the Services under and in accordance with the Agreement ("Users") • Any other data subject(s) whose Personal Data is submitted to the Services by or on behalf of Third Party Controllers' staff.

Annex 2

Security Measures

As from the Addendum Effective Date, SupplyPro will implement and maintain the Security Measures set out in this Annex 2.

1. Data Center and Network Security

(a) Data Centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow SupplyPro to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Businesses Continuity. SupplyPro has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks and Transmission.

Data Transmission. Data centers are typically connected via high-speed links to provide secure and fast data transfer. SupplyPro transfers data via Internet standard protocols.

External Attack Surface. SupplyPro employs multiple layers of network devices and intrusion detection to protect its external attack surface. SupplyPro considers potential attack vectors and incorporates appropriate purpose-built technologies into external facing systems.

Incident Response. SupplyPro monitors a variety of communication channels for security incidents, and SupplyPro's security personnel will react promptly to known incidents.

Encryption Technologies. SupplyPro makes HTTPS encryption (also referred to as SSL or TLS connection) available.

2. Access and Site Controls

(a) Site Controls.

On-site Data Center Security Operation. SupplyPro's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor closed circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. SupplyPro maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. SupplyPro's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors,

shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site 24 hours a day, 7 days a week.

(b) Access Control.

Infrastructure Security Personnel. SupplyPro has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. SupplyPro's infrastructure security personnel are responsible for the ongoing monitoring of SupplyPro's security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. Data Owner and any relevant Third Party Controller administrators must authenticate themselves via a central authentication system or via a single sign on system in order to administer the Services.

3. Data

(a) Data Storage and Segregation. SupplyPro stores data in a multi-tenant environment on SupplyPro servers. SupplyPro logically segregates data belonging to different Data Owners or Third Party Controllers.

(b) Decommissioned Disks and Disk Erase Policy. Disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving SupplyPro's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by independent validators. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

4. Personnel Security

SupplyPro personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. SupplyPro conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, SupplyPro's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Personal Data are required to complete additional requirements appropriate to their role (e.g., certifications). SupplyPro's personnel will not process Personal Data without authorization.

SupplyPro may update or modify such Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

Annex 3

Subprocessors

Subprocessor	**Function**	**Location**	**Contact person's name, position and contact details**
Janus Networks	Technical Support Services	10225 Barnes Canyon Rd, #A101 San Diego, CA 92121	Nicholas Chu, Owner, nchu@janusnetworks.com
datAvail	Technical Support Services	11800 Ridge Parkway, Suite 125 Broomfield, CO 80021	Michael Eversole, National Account Executive michael@datAvail.com
Crowdstrike	Technical Support Services	150 Mathilda Place, Suite 300 Sunnyvale, CA 94086	David Palanivk, Account Manager David.palanivk@crowdstrike.com

Annex 4

Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 –Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules Two and Three: Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

[NOT USED]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life

or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION **[NOT USED]**

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fourteen (14) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION **[NOT USED]**

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least fourteen (14) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

For Module Three: The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date: these clauses are hereby deemed to be entered into by the data exporter under and in accordance with Section 8.2 of the Data Protection Addendum into which these Clauses are incorporated.

Role (controller/processor):

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

1. Name: SupplyPro, Inc.

Address: 9401 Waples Street, Ste. 150, San Diego, CA 92121

Contact person's name, position and contact details: Luciano Nery, Customer Support Manager, 858-587-6400

Activities relevant to the data transferred under these Clauses: Provision of the Services as described in the Agreement and Data Protection Addendum into which these Clauses are incorporated.

Signature and date: these clauses are hereby deemed to be entered into by the data importer under and in accordance with Section 8.2 of the Data Protection Addendum into which these Clauses are incorporated.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

As described in Annex I to the Data Protection Addendum into which these Clauses are incorporated.

Categories of personal data transferred

As described in Annex I to the Data Protection Addendum into which these Clauses are incorporated.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

As initiated by the Data Owner or applicable Third Party Controller in using the Services.

Nature of the processing

Processing in the course of the provision of the Services as described in the Agreement and the Data Protection Addendum into which these Clauses are incorporated.

Purpose(s) of the data transfer and further processing

For the purpose of the provision of the Services as described in the Agreement and the Data Protection Addendum into which these Clauses are incorporated.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the period determined in accordance with the Agreement and the Data Protection Addendum into which these Clauses are incorporated.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Onward transfers to subprocessors as described in Annex 3 to the Data Protection Addendum into which these Clauses are incorporated.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13.

The competent supervisory authority shall be determined as follows:

- Where the data exporter is established in an EU Member State: the competent supervisory authority shall be the supervisory authority of that EU Member State in which the data exporter is established.
- Where the data exporter is not established in an EU Member State, Article 3(2) of the GDPR applies and the data exporter has appointed an EU representative under Article 27 of the GDPR: the competent supervisory authority shall be the supervisory authority of the EU Member State in which the data exporter's EU representative relevant to the processing hereunder is based (from time-to-time).
- Where the data exporter is not established in an EU Member State, Article 3(2) of the GDPR applies, but the data exporter has not appointed an EU representative under Article 27 of the GDPR, the competent supervisory authority shall be the supervisory authority of the EU Member State notified in writing to [dgilger@supplypro.com], which must be an EU Member State in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Please refer to Annex 2 to the Data Protection Addendum into which these Clauses are incorporated.

Subprocessors: When SupplyPro engages a Subprocessor under these Clauses, SupplyPro shall enter into a binding contractual arrangement with such Subprocessor that imposes upon them data protection obligations which, in substance, meet or exceed the relevant standards required under these Clauses and the Data Protection Addendum into which these Clauses are incorporated. For the purposes of Clause 10, the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance in respect of data subject requests shall be provided, as well as the scope and the extent of the assistance required, is: provided via self-service functionality within the Services, which enables Data Owners to change or delete Personal Data by following the steps set out below:

- Log into SSIS at https://supplysystem.supplypro.com/ClientSite/Home
- Navigate to 'Partners' or 'Clients' (as applicable) in the drop-down
- When you are in the company group, navigate to 'Users'
- Find a name in the column 'USER NAME'
- To Edit or Delete Personal Information
    - To Change/Edit a User's Personal information:
        - Select the EDIT icon in the ACTION column, which will open up ACCOUNT DETAILS, CONTACT DETAILS and AREAS Sections
        - Edit details as appropriate in any of the above sections
        - Select the SAVE button at the bottom of the page

- To Delete a User and their Personal information:
  - Select the EDIT icon which will open up ACCOUNT DETAILS, CONTACT DETAILS and AREAS Sections
  - Erase all information fields that are populated, ie, email, first name, phone, Mobile, job title, etc.
  - Replace the Last Name and Login fields with some other value, such as, 'Requested Removal' or 'Deleted User', as this User (User Name, Login) will still show up on scheduled reports
  - Select the SAVE button at the bottom of the page
  - Go back to the ADMINISTRATION area/User Search
  - Select the DELETE icon for this new User Name and Login
  - Confirmation – Select either Cancel or OK as confirmation of 'Are you sure you want to delete?'

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

The Parties acknowledge and agree that this Annex III is not applicable on the basis that general authorisation of subprocessors, as opposed to specific authorisation of subprocessors, is granted pursuant to Clause 9(a), Option 2.