STANDARD CONTRACTUAL CLAUSES (A28)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5

Docking Clause

Intentionally left blank

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1 Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.

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

7.5 Sensitive data

If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

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

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time

to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

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

7.8 International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7 for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

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

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

LIST OF PARTIES

Controller(s):

Name: Customer as listed in the applicable Order Form

Address: See the applicable Customer Order Form

Contact person's name, position and contact details: See the applicable Customer Order Form

Signature and accession date: Execution of the applicable Order Form by the controller includes execution of these Clauses, which are countersigned by the processor

The controller enters into these Clauses on behalf of itself and, to the extent required under the Regulation (EU) 2016/679, in the name and on behalf of its Authorized Affiliates, if and to the extent the processor processes personal data for which such Authorized Affiliates qualify as the controller. For the purpose of these Clauses, "***Authorized Affiliate***" means any Customer Affiliate which is subject to the Regulation (EU) 2016/679 and is permitted to use the Subscription Service or Professional Services pursuant to the Master Subscription and Professional Services Agreement and related Order Form or SOW signed between the controller and the processor ("***Agreement***"), but has not signed its own Order Form or SOW, and is not a 'Customer' as defined under the Agreement. An Authorized Affiliate(s) may exercise its rights and enforce the terms of these Clauses directly against the processor, subject to the following:

- except where Regulation (EU) 2016/679 or these Clauses require that the Authorized Affiliate itself exercise a right or enforce a claim, the controller will exercise any such right or claim directly against the processor on behalf of such Authorized Affiliate; and
- the controller will exercise any rights under these Clauses in a combined manner for itself and all Authorized Affiliates together rather than separately.

Processor(s):

Name: PROS France SAS

Address: 185 rue Galilee, 31670 Labège, France

Contact person's name, position and contact details: privacy@pros.com

Signature and accession date: Chris Chaffin 22 November 2022

ANNEX II

DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed and Categories of personal data processed

The controller may submit personal data to the Subscription Service, the extent of which is determined and controlled by the controller in its sole discretion. Depending on the use case, this may include, but is not limited to, the following categories of personal data and data subjects:

Smart Configure, Price, Quote & Smart Price Optimization and Management Solutions		
Subscription Service	**Categories of Personal Data**	**Categories of data subjects**
• **Smart Configure, Price, Quote (Essentials/ Advantage /Ultimate)** • **PROS Smart CPQ**	• User log-in ID and credentials • First and last name • Title, Position and Employee ID • Employer • Email address • Phone number	• Users of the Subscription Service
	This will depend on your configuration, but may include: • First and last name • Title and Position • Employer • Email address • Phone number • Address • Certain Personal Life Data to the extent necessary to perform the configure, quote process	• Prospects and customers of Customer and Customer Affiliates
• **Smart Price Optimization and Management (Essentials/ Advantage /Ultimate)** • **PROS Control** • **PROS Guidance** • **PROS Opportunity Detection**	• User log-in ID and credentials • First and last name • Title, Position and Employee ID • Employer • Email Address • Phone Number	• Users of the Subscription Service
• **PROS Contribution Management System (CMS)**	• User log-in ID and credentials • First and last name • Title and position • Employer • Email address	• Users of the Subscription Service
Travel Solutions		
Subscription Service	**Categories of Personal Data**	**Categories of data subjects**
• **PROS RM (Essentials/ Advantage)** • **PROS RM Essentials Network Add-On** • **PROS Market Valuation Module (MVM)**	• User log-in ID and credentials • First and last name • Employer • Title and Position • Email address	• Users of the Subscription Service
• **PROS Group Sales Optimizer (GSO) (Advantage/ Ultimate/ Essentials)**	• User log-in ID and credentials • First and last name • Employer • Title and Position • Email address • Physical business Address • Phone number	• Users of the Subscription Service • Customer (and Customer Affiliates') business partners and resellers, as well as their employees and other related persons

	• First and last name • Date of birth • PNR locator (booking reference number) • Travel information (e.g., destination, fare information, travel status)	• Prospects and customers of Customer and Customer Affiliates
• **PROS Real-Time Dynamic Pricing (RTDP) (Advantage/ Ultimate)**	• User log-in ID and credentials • First and last name • Employer • Email address	• Users of the Subscription Service
• **PROS Dynamic Offers**	• User log-in ID and credentials • First and last name • Title and Position • Employer • Email address	• Users of the Subscription Service • Customer (and Customer Affiliates') business partners and resellers, as well as their employees and other related persons
	• Dynamic Offers processes certain pseudonymous data - such as date of birth, bank identification number, gender, country of citizenship and residence, and frequent flyer program details (e.g. miles accumulated, passenger score/tier level) – where the additional information required to identify the individual is held by Customer (or its business partners and resellers)	• Prospects and customers of Customer and Customer Affiliates
• **PROS Pricing Cache**	• User log-in ID and credentials • First and last name • Employer • Title and Position • Email address	• Users of the Subscription Service • Customer (and Customer Affiliates') business partners and resellers, as well as their employees and other related persons
• **PROS Digital Retail**	• First and last name • Email address & phone number • Date of birth (for minors only) • Meal preferences • Health data if relevant to travel requirements • Certain additional information dependent on destination (e.g. gender, date of birth, travel document number, issue country, redress number and known traveler number) • Online identifiers (IP address, website clicks)	• Users of the Subscription Service, which include prospects and customers of Customer and Customer Affiliates
"***Users***" mean Customer's employees, consultants, clients, external users, contractors, agents or other third parties authorized to use the Subscription Service by Customer and have been assigned unique user identifications and passwords.		

Sensitive data processed (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.

This will depend on the use case for the Subscription Service. The controller may submit special categories of data to the Subscription Service and/or as part of the Professional Services, the extent of which is determined and controlled by the controller in its sole discretion. Please see Annex II for details of the restrictions and safeguards applied by the processor to all Customer data.

Nature of the processing

The processing will be carried out in accordance with the Agreement between the controller and the processor, and any documented instructions given by the controller.

Purpose(s) for which the personal data is processed on behalf of the controller

The processor operates a global support network and operations facilities and processing may take place in any jurisdiction where the processor or its sub-processors operate such facilities. The processor will process personal data for the purposes of providing the Subscription Service and Professional Services as specified in the Agreement.

Duration of the processing

The processing will be carried out for the Subscription Term designated in the applicable Customer Order Form to which these Clauses are annexed

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

As per the above.

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

Throughout the Subscription Term, the processor will maintain a security program that meets or exceeds the controls set forth in the processor's (i) most recently completed SOC1 and SOC2 audit reports (or comparable industry-standard successor reports prepared by the processor's independent third-party auditor), and (ii) Security Exhibit that is designed to protect the security, confidentiality and integrity of Customer Data. The processor's Security Exhibit can be accessed at https://pros.com/pros-security-exhibit.

The processor will not diminish the protections provided by the controls set forth in the Audit Report and Security Exhibit. These protections include:

ISMS: PROS will maintain an Information Security Management System that defines PROS policies, standards, guidelines, and procedures as part of PROS documented information security program covering the management of information security for the Subscription Services and all related PROS internal operations. PROS ISMS is designed to:

- Establish directives and principles for action regarding information security;
- Document and maintain compliance with statutory, regulatory, and contractual requirements, including SOC1, SOC2, SOX, GDPR, CCPA, CSA STAR, ISO 27001, and ISO 27018; and
- Monitor, evaluate and adjust, as appropriate, considering relevant changes in technology, threats to PROS or to Customer data and security and privacy regulations applicable to PROS.

Access Control. PROS ISMS will include policies, procedures and logical controls designed to restrict access to PROS networks, PROS systems and all elements of the Subscription Service (including Customer data) on a need-to-know basis and based on the principle of "least privilege". PROS will (i) electronically monitor and manage active access privileges; (ii) verify business justification for access requests; (iii) limit duration of access; and (iv) promptly remove access in the event of a change in job responsibilities, job status or otherwise when access is no longer needed. PROS will secure access points via the use of unique identifiers, password complexity, regularly scheduled password updates and, where PROS deems appropriate, multi-factor authentication (MFA).

Encryption. PROS ISMS will include policies, procedures and logical controls designed to enforce encryption on all externally accessible systems and communications. PROS will: (i) administer encryption protocols designed to isolate network communication between application host and database host; (ii) provide access to the internet-facing PROS web port (for HTTPS) through network firewalls, (iii) secure volume-based encryption of data-at-rest using keys stored separately from the data; and (iv) secure all end points using encryption, password protection and remote deactivation capability.

Change Management. PROS ISMS will include a change management program to govern all changes to PROS production Subscription Service systems, applications, and databases, including (i) documentation, testing, and approval of all changes; (ii) security assessments of all changes prior to deployment into production; and (iii) security patching in a timely manner based on risk analysis. In addition, PROS will require all changes to Customer production environments to be documented on an approved change request prior to deployment.

Testing. At least annually, PROS will review and test key controls, systems, and procedures of PROS ISMS to validate that they are properly implemented and effective in addressing identified threats and risks.

Business Continuity & Disaster Recovery. PROS ISMS will include a business continuity framework designed to mitigate the risk of single points of failure and provide a resilient environment to support Subscription Service continuity and performance. PROS will administer comprehensive plans for crisis management and communication, supply chain

management and individualized department action strategies designed to prevent interruption of critical business functions. PROS will also administer formal disaster recovery plans designed to minimize disruption to critical business operations and Customer systems. PROS will maintain production and disaster recovery environments to support failover procedures and redundancy requirements, as well as proactive protection and detection methods designed to limit damage from disaster events.

Incident Response. PROS ISMS will include a security incident response plan to be followed in the event of any unauthorized exposure, corruption, or loss of Customer data (each a "***Security Incident***"). Such Security Incident response plan will, at a minimum, define personnel roles and responsibilities, as well as procedures related to Security Incident identification, containment, investigation, communication, forensic analysis, recovery and remediation, documentation, and reporting. If PROS verifies that any Customer data is impacted by a confirmed Security Incident, PROS will notify the affected Customer without undue delay to the extent permitted by law.

Responding to Governmental Access Requests: Although PROS views it as extremely unlikely, if PROS is subject to a government data access request, it will respond as follows:

- PROS will first review the disclosure request to ensure it is valid and legally binding. No disclosure will be made except in response to a valid and legally binding order.
- PROS will promptly notify the applicable Customer of the request (unless prohibited from doing so, in which case PROS will provide the Customer with as much relevant information as lawfully possible on the request) and try to redirect the request directly to Customer.
- If PROS is prohibited from notifying Customer of the request, PROS will use its best efforts to have the prohibition lifted and notify Customer as soon as legally permitted.
- If disclosure is compelled, PROS will only disclose the minimum amount of data necessary for compliance.
- If, following a review of the legality of the request, PROS concludes that the request is unlawful, PROS will, where appropriate, challenge the request and pursue available possibilities of appeal.
- Unless legally required, PROS will not provide bulk access to data, and will not provide access to Customer personal data on a voluntary basis.
- Where legally permissible and when requested, PROS will provide Customer with a summary of any law enforcement access requests it has received.
- Where legally permissible, PROS will document and record any law enforcement access request and PROS respective response, and provide such documentation to Customer to the extent (a) the request relates to Customer's personal data; and (b) provision of documentation is legally permissible.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller

The sub-processor provides technical and organizational measures that ensure the same level of assistance to the controller as those provided by the processor.

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.

As per above.

ANNEX IV: SUB-PROCESSORS

The list of authorized sub-processors and authorized transfers of personal data is available at processor's Customer Portal, PROS Connect, https://pros.com/subprocessor-list. Alternatively, please contact your Customer Success Manager for a copy.

The processor will inform the controller in advance of any intended additions or replacements to the list of sub-processors by sending an alert to the controller's designated contact(s) through PROS Connect Portal. The controller may subscribe to notifications of new sub-processors for those Subscription Services for which the controller has a then-current active subscription through PROS Connect.

If the controller has legitimate reason under these Clauses to object to a new sub-processor, the controller shall promptly, and in any event within 14 days of the processor's alert, provide notice of such objection by sending an email to the processor at privacy@pros.com. If the controller objects, the processor and the controller will discuss a commercially reasonable resolution. If no commercially reasonable resolution can be reached within 30 days from the processor's initial notification of the new sub-processor, the controller will have an additional 5-day period during which time it may by written notice terminate the relevant Order Form to the extent that it requires use of the proposed sub-processor. If the controller does not object within the initial 14-day period, the controller is deemed to have accepted the new sub-processor.

ANNEX V: CLARIFICATIONS REGARDING THE AUDIT PROCESS

Clause 7.6: Documentation and compliance (c), (d), (e)

The controller agrees that the processor's most recently completed SOC1 and SOC2 audit reports, or comparable industry-standard successor reports, prepared by the processor's independent third-party auditor will, to the extent applicable, be used to satisfy any audit or inspection requests by or on behalf of the controller, and the processor will make such reports available to the controller upon request. These reports will be subject to the confidentiality obligations set forth in the Agreement.

If the controller, its independent auditor, or a Supervisory Authority requests an on-site audit of procedures relevant to the processing of personal data by the processor, the processor will contribute to such audits as follows:

- the controller gives the processor reasonable written notice of any audit, which shall not be less than 30 days (unless a Supervisory Authority requires shorter notice, or a personal data breach has occurred);
- the scope of the audit is mutually agreed between the parties acting reasonably and in good faith;
- the audit is conducted during the processor's regular business hours and at reasonable intervals, and in any event no more than once per calendar year (unless the audit is required or requested by a Supervisory Authority); and
- the controller bears the costs of the audit unless the audit reveals a material breach by the processor of these Clauses, then the processor shall bear its own expenses of an audit.

Reports following from the audit or inspection will be treated as the processor's confidential information and subject to the confidentiality obligations of the Agreement. The controller may disclose these reports to a Supervisory Authority if so requested. The controller shall promptly notify the processor and provide information about any actual or suspected non-compliance discovered during an audit, which the processor will promptly remedy at its own cost.

ANNEX VI: PROCESSING OF UK PERSONAL DATA

This section will apply to the extent there is any processing of personal data that is subject to the UK GDPR or the UK GDPR applies to the processor or the controller ("**UK Data**"). The UK GDPR means Regulation (EU) 2016/679 as implemented into the law of the United Kingdom by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 and the Data Protection Act 2018 (and as further amended).

The Parties agree that the Clauses shall be interpreted to take effect under the UK GDPR with respect to UK Data as follows:

- references to Article 28(3) and (4) of Regulation (EU) 2016/679 will be deemed to refer to Article 28 of the UK GDPR and references to Regulation (EU) 2016/679 to the UK GDPR.
- references to the Supervisory Authority will be deemed to refer to the Information Commissioner's Office.
- references to Union or Member State law will be deemed to refer to UK law.
- annexes I, II, III, IV and V of the Clauses will apply to the processing of UK Data.

This Annex VI shall be interpreted in a manner that is consistent with the UK GDPR and so that it fulfils the Parties' obligation to comply with Article 28 UK GDPR.

ANNEX VII: PROCESSING OF SWISS PERSONAL DATA

This section will apply to the extent there is any processing of Swiss personal data subject to the Swiss Federal Act on Data Protection (FADP) ("**Swiss Data**").

The Parties agree that the Clauses shall be interpreted to take effect under the FADP with respect to Swiss Data as follows:

- references to the GDPR should be understood as references to the FADP.
- for so long as required under the FADP, the personal data of legal entities shall be protected pursuant to these Clauses.
- references to the Supervisory Authority will be deemed to refer to the Federal Data Protection and Information Commissioner (FDPIC).
- annexes I, II, III, IV and V of the Clauses will apply to the processing of Swiss Data.