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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) 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

Intentionally left blank

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.

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.

Clause 9

Use of sub-processors

(a) 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 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.

Clause 10

Data subject rights

(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.

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.

(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

(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

(a) 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.

(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

(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;

(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).

(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. 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 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

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.

(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.).

(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.

(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 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

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

(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

ANNEX I

A. LIST OF PARTIES

Data exporter(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

Activities relevant to the data transferred under these Clauses: The data exporter is purchasing PROS cloud solutions and related professional services

Signature and date: Execution of the applicable Order Form by the data exporter includes execution of these Clauses, which are countersigned by PROS, Inc.

Role (controller/processor): Controller. The data exporter 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 data importer 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 data exporter and the data importer ("***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 data importer, 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 data exporter will exercise any such right or claim directly against the data importer on behalf of such Authorized Affiliate; and
- the data exporter will exercise any rights under these Clauses in a combined manner for itself and all Authorized Affiliates together rather than separately.

Data importer(s):

Name: PROS, Inc.

Address: 3200 Kirby Drive, Suite 600, Houston, Texas 77098, USA

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

Activities relevant to the data transferred under these Clauses: The data importer is a global provider of software as a service solutions, including global support services, and related professional services.

Signature and date: Chris Chaffin

18 October 2021

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

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

The data exporter may submit personal data to the Subscription Service, the extent of which is determined and controlled by the data exporter 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**
• **PROS Smart Configure, Price, Quote (Essentials/ Advantage /Ultimate)** • **PROS Smart CPQ**	• User log-in ID and credentials • Online identifiers (IP address) • Location data (time zone, location/language preferences) • First and last name • Title, Position and Employee ID • Employer • Email address • Phone number • Business address	• 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 • Location data (time zone, location/language preferences) • Certain Personal Life Data to the extent necessary to perform the configure, quote process	• Prospects and customers of Customer and Customer Affiliates
• **PROS Smart Price Optimization and Management (Essentials/ Advantage /Ultimate)** • **PROS Control** • **PROS Guidance** • **PROS Integrate** • **PROS Real-Time Pricing Engine (RTPE)** • **PROS Opportunity Detection**	• User log-in ID and credentials • Location data (time zone, location/language preferences) • Online identifiers (IP address) • 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)**	• 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 Retail for Airlines**	• 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 individuals who are authorized by the data exporter to use the Subscription Service, subject to the terms of the Agreement, and have been supplied user identifications and passwords by the data exporter. Users may include, for example, data exporter's and its Affiliates' employees, consultants, clients, external users, contractors, agents and authorized third parties.		

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.

This will depend on the use case for the Subscription Service. The data exporter 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 data exporter in its sole discretion. Please see Annex II for details of the restrictions and safeguards applied by the data importer to all Customer personal data.

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

The data is transferred on a continuous basis as required to provide the Subscription Service and related Professional Services.

Nature of the processing

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

Purpose(s) of the data transfer and further processing

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

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

The personal data will be retained for the Subscription Term designated in the applicable Customer Order Form to which these Clauses are annexed. Upon expiration or termination of the data exporter's use of the Subscription Service or Professional Services, it will have a 30-day period within which it may request a copy of Customer data and thereafter, the data importer will delete all Customer data, including personal data, in accordance with the applicable terms of the Agreement.

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

As per the above.

C. COMPETENT SUPERVISORY AUTHORITY

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

Where the data exporter/Customer signing the applicable Order Form is located within the EU (based on the Customer's address in the applicable Order Form), the competent authority shall be the Supervisory Authority of that Member State. If the data exporter/Customer signing the applicable Order Form is not located within the EU, the competent authority shall be the Irish Supervisory Authority.

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

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

The data importer 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 and, for transfers from a processor to a sub-processor, to the data exporter

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

ANNEX III –SUB-PROCESSORS

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

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

If the data exporter has legitimate reason under these Clauses to object to a new sub-processor, the data exporter shall promptly, and in any event within 14 days of the data importer's alert, provide notice of such objection by sending an email to the data importer at privacy@pros.com. If the data exporter objects, the data importer and the data exporter will discuss a commercially reasonable resolution. If no commercially reasonable resolution can be reached within 30 days from the data importer's initial notification of the new sub-processor, the data exporter 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 data exporter does not object within the initial 14-day period, the date exporter is deemed to have accepted the new sub-processor.

ANNEX IV –CLARIFICATIONS REGARDING THE AUDIT PROCESS

Clause 8.9: Documentation and compliance (c), (d), (e)

The data exporter agrees that the data importer's most recently completed SOC1 and SOC2 audit reports, or comparable industry-standard successor reports, prepared by the data importer'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 data exporter, and the data importer will make such reports available to the data exporter upon request. These reports will be subject to the confidentiality obligations set forth in the Agreement.

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

- the data exporter gives the data importer 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 data importer'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 data exporter bears the costs of the audit unless the audit reveals a material breach by the data importer of these Clauses, then the data importer shall bear its own expenses of an audit.

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

ANNEX V –SWISS GDPR ADDENDUM

This Addendum amends the Clauses to work in the context of Swiss data transfers.

- In so far as the data transfers are subject to the FADP, references to the GDPR should be understood as references to the Swiss Federal Act on Data Protection (FADP).

- For so long as required under the FADP, the personal data of legal entities shall be protected pursuant to these Clauses.

- **Clause 13: Supervision:** Parallel supervision:
    - Where the data transfer is governed by the FADP: the Federal Data Protection and Information Commissioner (FDPIC) is the competent supervisory body;
    - Where the data transfer if governed by GDPR: the criteria of Clause 13a shall apply
- **Clause 18(c): Choice of forum and jurisdiction:** A data subject, who has his/her habitual residence in Switzerland, may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland.