DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is entered into between Patsnap (UK) Ltd, on behalf of itself and its affiliates, an entity incorporated in the United Kingdom having offices at 30 Stamford Street Wework, 6th Floor, London, England, SE1 9LQ ("PatSnap"), and the undersigned entity ("**Customer**"). This DPA is effective on the date that the applicable Agreement has been duly executed by both parties. In signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required by Data Protection Law, its affiliates. Capitalized terms not otherwise defined herein shall have the meanings set forth in Section 1.

HOW THIS DPA APPLIES

This DPA is only valid and legally binding if the Customer is: (a) a party to an Agreement subject to which PatSnap is a data processor for the purposes of GDPR and/or a Service Provider for the purposes of CCPA; and (b) a data controller to which Article 3 of GDPR applies, or a Business for the purposes of CCPA. This DPA forms part of such Agreement. If multiple Agreements exist between the parties, a separate instarnce of this DPA shall apply with respect to each Agreement.

1. DEFINITIONS

"**Agreement**" means any agreement between PatSnap and the Customer or between the Customer and a PatSnap-authorized partner under which Products are provided by PatSnap and/or a PatSnap-authorized partner to the extent PatSnap is processing Personal Data under such agreement between Customer and such PatSnap-authorized partner.

"**CCPA**" means the California Consumer Privacy Act of 2018.

"**controller**", "**data subject**", "**personal data**", "**personal data breach**," "**process**", "**processing**", "**processor**", and "**supervisory authority**" have the same meanings as in GDPR. "**Business**" and "**Service Provider**" shall have the same meanings as in CCPA.

"**Data Protection Law**" means GDPR, CCPA, Data Protection Act 2018, any and all applicable national data protection laws and regulations, and any and all laws and regulations of the European Union and/or the European Economic Area the ("**EEA**") or elsewhere, to the extent applicable to the processing of Personal Data under the Agreement, as amended or replaced from time to time.

"**GDPR**" means the General Data Protection Regulation (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.

"**Personal Data**" means personal data that is submitted to PatSnap by Customer and processed by PatSnap and/or its Sub-processors (as hereinafter defined) for the purposes of providing the Products to Customer.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration,unauthorized disclosure of, or access to, Customer Personal Data processed by PatSnap under this DPA.

"**Products**" means the PatSnap services and products ordered, subscribed, or licensed by Customer in an Agreement, including software, technical support and professional services as set out in the applicable Agreement.

"**Standard Contractual Clauses**" or **"Clauses"** means the Standard Contractual Clauses based on the Commission Decision (EU) 2021/915 Standard Contractual Clauses (processors) document attached hereto as Exhibit A or any

such clauses amending, replacing or superseding those by a European Commission decision or by a decision made by any other authorized body.

2. DATA PROCESSING

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the processing of Personal Data, Customer is the controller and PatSnap is the processor and that PatSnap will engage Sub-processors pursuant to the requirements set forth in Section 5 below. The parties agree that they shall comply with Data Protection Law as applicable to them in such roles.

2.2 Processing of Personal Data. PatSnap shall, in its delivery of the Products and provision of instructions, process Customer's Personal Data in accordance in all material respects with the requirements of applicable Data Protection Law. Customer shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Customer acquired Personal Data and transferred such Personal Data to PatSnap.

2.3 PatSnap Processing of Personal Data. As Customer's processor, PatSnap shall only process personal data for the following purposes: (a) processing in accordance with the Agreement; (b) processing initiated by Customer or its authorized users in their use of the Products; and (c) processing to comply with other reasonable documented instructions of Customer (e.g. via email or via the support portal) that are consistent with the terms of the Agreement (individually and collectively the "**Purpose**"). PatSnap shall inform Customer immediately upon becoming aware that, in PatSnap's opinion, an instruction provided by Customer violates applicable Data Protection Law.

2.4 Details of the Processing. The subject matter of processing of Personal Data by PatSnap is described in the Purpose set out in Section 2.2. The duration of the processing, the nature and purpose of the processing, the types of Personal Data and the categories of data subjects processed under this DPA are further specified in Exhibit C (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

PatSnap shall, to the extent legally permitted, promptly notify Customer if PatSnap receives any requests from a data subject to exercise the following individual rights under Data Protection Law in relation to the Personal Data: right of access, right to rectification, restriction of processing, erasure, data portability, objection to the processing, right not to be subject to an automated individual decision making (each a **"Data Subject Request"**), each to the extent such individual rights apply to a data subject under applicable Data Protection Law. Taking into account the nature of the processing, PatSnap will assist Customer insofar as such assistance is commercially reasonable for the fulfilment of Customer's obligation to respond to a Data Subject Request. To the extent that Customer, in its use of the Products, does not have the ability to adequately address a Data Subject Request, PatSnap shall, upon Customer's written request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent PatSnap is legally permitted to do so and the response to such Data Subject Request is required by applicable Data Protection Law. To the extent legally permitted, Customer shall be responsible for any cost arising from PatSnap's provision of such assistance including costs or fees associated with provision of additional functionality.

4 SUB-PROCESSORS

4.1 Use of Sub-processors. Customer acknowledges and agrees that PatSnap shall use third party sub-contractors to process Personal Data in some circumstances, which may include PatSnap's affiliates ("**Sub-processors**"). Customer consents to PatSnap's use of Sub-processors. Customer acknowledges that PatSnap is involved in the provision of the Products to Customer either directly or through the provision of support to PatSnap's affiliates. In either case Customer agrees to enter into the Standard Contractual Clauses set out in Exhibit C and acknowledges that Sub-processors may be appointed by PatSnap in accordance with Clause 11 of Exhibit C.

4.2 Liability. PatSnap will: (a) enter into a written agreement with any Sub-processor containing terms that are no less protective of Personal Data than those contained in this DPA; and (b) be liable for the acts and omissions of its Sub-processors to the same extent PatSnap would be liable if performing the services of each of those Sub-processors directly under the terms of this DPA.

5. SECURITY

PatSnap shall maintain appropriate technical and organizational measures to protect the security, confidentiality and integrity of Personal Data against a Personal Data Breach as set forth in Exhibit B. Such measures will take into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk to the rights and freedoms of natural persons so as to ensure a level of security that is appropriate to the risk. PatSnap regularly monitors compliance with these technical and organizational measures and may amend them from time to time provided that PatSnap maintains at least an equivalent level of protection. Upon Customer's written request, PatSnap will provide an updated description of PatSnap's technical and organizational measures, to the extent applicable, in the form presented in Exhibit B. All PatSnap personnel who process Personal Data shall be adequately trained with respect to their data protection, security and confidentiality obligations, and shall be subject to written obligations to maintain confidentiality.

6. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

PatSnap shall notify the Customer within 72 hours after confirming the occurrence of a breach relating to Personal Data (within the meaning of applicable Data Protection Law) which may require a notification to be made to any supervisory authority or data subject under applicable Data Protection Law or which PatSnap is required to notify to Customer under applicable Data Protection Law (a "**Personal Data Incident**"). PatSnap shall provide commercially reasonable cooperation and assistance in identifying the cause of the Personal Data Incident and take commercially reasonable actions to mitigate the effects of the Personal Data Incident and remediate the cause, to the extent such remediation is within PatSnap's control. Except as required by applicable Data Protection Law, this shall not apply to incidents that are caused by Customer, Customer's authorized users, and/or any products or services not provided by PatSnap.

7. RETURN AND DELETION OF PERSONAL DATA

Upon termination of the Agreement, PatSnap shall delete the Personal Data from its systems in accordance with the terms of that Agreement and at all times subject to applicable Data Protection Law. If immediate deletion is not possible (e.g. because some data is archived or stored in back up files), PatSnap shall ensure that no further processing of such data takes place after termination of the Agreement and shall move it for full deletion as soon as possible, no later than 45 days following termination of the Agreement. PatSnap may maintain one copy of any data which is required by law to be kept, for example for the purposes of auditing financial records.

8. EU SPECIFIC PROVISIONS

8.1 GDPR. PatSnap will process Personal Data in accordance with GDPR requirements directly applicable to PatSnap's provision of the Products sold, licensed or provided to Customer. Upon Customer's written request, PatSnap shall provide Customer with commercially reasonable cooperation and assistance reasonably necessary to fulfil Customer's obligation under GDPR to carry out a data protection impact assessment related to Customer's use of the Products, to the extent that Customer does not already have access to the relevant information, PatSnap does have access to the relevant information, and the data protection impact assessment is required by Data Protection Law.

8.2 International Data Transfers. The Customer acknowledges and agrees that regardless of the location in which Personal Data is stored, Personal Data may be transferred to other jurisdictions (including outside of the EEA): (i) in order to provide technical and customer support, account management, billing and other ancillary functions, and (ii) as

expressly described in the Agreement or this DPA. PatSnap shall not transfer Personal Data to (nor permit Personal Data to be processed in or from) a country outside of the EEA unless it takes such measures as are necessary to ensure that the transfer is in compliance with applicable Data Protection Law. Where Personal Data is transferred from a processor within the EEA to a processor outside of the EEA in any country: (a) not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the applicable Data Protection Law), and (b) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, the Standard Contractual Clauses contained in Exhibit A shall apply to such transfer.

9. CALIFORNIA SPECIFIC PROVISIONS

9.1 CCPA. This Section 9 applies to PatSnap's processing of Personal Data that is subject to CCPA.

9.2 Permitted Use. PatSnap shall not retain, use or disclose Personal Data for any purpose other than the Purpose, or as otherwise permitted by CCPA, including retaining, using or disclosing the Personal Data for a commercial purpose other than providing the Services specified in the Agreement.

9.3 Selling Prohibited. PatSnap shall not sell Customer's Personal Data as the term "sell" is defined by CCPA.

10. GENERAL

10.1 Term and Termination. This DPA will remain in force until (i) it is replaced or repealed by mutual agreement of Customer and PatSnap, or (ii) the Agreement is terminated or expires.

10.2 Modification. Any modification to this DPA shall be invalid unless made in writing and signed by both parties.

10.3 Liability. Any claims brought under this DPA will be subject to the same terms and conditions, including the exclusions and limitations of liability, as are set out in the Agreement. The total liability of PatSnap and its affiliates for all claims by Customer arising out of or related to the Agreement and this DPA shall apply in aggregate for all claims under both the Agreement and this DPA.

10.4 Governing Law. Without prejudice to clause 7 (Mediation and Jurisdiction) and clause 9 (Governing Law) of the Standard Contractual Clauses: (i) the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and (ii) this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

10.5 Counterparts. This DPA may be executed in any number of counterparts, each of which will be deemed to be an original and all of which taken together will comprise a single instrument. This DPA may be delivered by electronic document format (e.g. PDF), and electronic copies of executed signature pages will be binding as originals.

10.6 Entire Agreement. This DPA, together with the Agreement, constitutes the entire agreement between the parties and supersedes any other prior or contemporaneous agreements or terms and conditions, written or oral, concerning the processing of Personal Data by PatSnap on behalf of Customer. In case of conflict or inconsistency between this DPA, the Agreement, and the Standard Contractual Clauses, the following order of precedence shall govern to the extent of the conflict or inconsistency: (i) the Standard Contractual Clauses; (ii) this DPA; and (iii) the Agreement.

10.7 Severability. If any provision of this DPA is determined to be unenforceable by a court of competent jurisdiction, that provision will be severed, and the remainder of terms will remain in full effect.

IN WITNESS WHEREOF, this DPA is made and entered into by duly authorized representatives of the parties as of the date set forth below.

PATSNAP:		**CUSTOMER:**
PATSNAP (UK) LTD		[_____]
Signature: _____		Signature: _____
Print name:		Print name:
Title:		Title:
Address:	3rd Floor, Building 11, Chiswick Business Park, 566 Chiswick High Road, London, W4 5YS	Address:
Date:		Date:

Exhibit A - 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) ([1]) 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

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 ([4]) (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) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] 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. ([8]) 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. The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

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

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

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

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance

with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

(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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

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 _____ (*specify Member State*).

(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.

ANNEX I

A. LIST OF PARTIES

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

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Activities relevant to the data transferred under these Clauses: …

   Signature and date: …

   Role (controller/processor): …

2. …

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

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Activities relevant to the data transferred under these Clauses: …

   Signature and date: …

   Role (controller/processor): …

2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

…

Categories of personal data transferred

…

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.

...

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

...

Nature of the processing

...

Purpose(s) of the data transfer and further processing

...

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

...

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

...

C. COMPETENT SUPERVISORY AUTHORITY

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

...

ANNEX II

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

XPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers. Patsnap technical and organisational measures are also defined in Exhibit B.

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

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

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

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2. …

Exhibit B
PatSnap Technical and Organizational Measures

1. INTRODUCTION

This Technical and Organizational Data Security Measures document articulates the technical and organizational security measures implemented by PatSnap in support of its Security Framework.

2. ACCESS CONTROL

2.1 ACCESS CONTROL OF PROCESSING AREAS (PHYSICAL)

Web applications, communications and database servers of PatSnap are located in secure data centers. PatSnap has implemented suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (telephones, database, application servers and related hardware) where Personal Data are processed or used, which includes the following:

- Establishing security areas.
- Protection and restriction of access paths.
- Securing the data processing equipment and personal computers.
- Establishing access authorizations for employees and third parties, including the respective documentation.
- Regulations and restrictions on card keys and fobs.
- Restricting physical access to the servers by using locked doors and separate cages within co-location facilities.
- Access to the data center where Personal Data are hosted is logged, monitored and tracked via electronic and CCTV video surveillance by security personnel.
- Data centers, where Personal Data may be hosted, are protected by security alarm systems and other appropriate security measures, such as user-related authentication procedures, including biometric authentication procedures (e. g. hand geometry) and/or electronic identity cards with users' photographs.

2.2 ACCESS CONTROL TO DATA PROCESSING SYSTEMS (LOGICAL)

PatSnap has implemented suitable measures to prevent its data processing systems from being used by unauthorized persons, which includes the following:

- Establishing the identification of the connected device to and/or the users of the PatSnap systems.
- Automatic session time-out when an admin user connection is left idle, which implies that identification and password are required to reopen.

- Automatic lock out of the admin user ID when several erroneous passwords are entered.
- Events are logged and logs are reviewed on a regular basis.
- Utilizing firewall, router and VPN-based access controls to protect the private service networks and back-end servers.
- Continuously monitoring infrastructure security.
- Regularly examining security risks by internal employees and third party auditors.
- Role-based access control implemented in a manner consistent with the principle of least privilege.
- Remote access to PatSnap's hosted network infrastructure is secured using two-factor authentication.
- Access to host servers, applications, databases, routers, switches, etc. is logged.
- Access and account management requests must be submitted through internal approval systems.
- Access must be approved by an appropriate approving authority. In most cases, the approval for a request requires two approvals at minimum: the employee's manager and the role approver or "owner" for the particular system or internal application.
- Passwords must adhere to the PatSnap password policy, which includes minimum length requirements, enforcing complexity and regular periodic resets.

PatSnap maintains Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS) and Security Incident and Event Management (SIEM) systems.

2.3 ACCESS CONTROL TO USE SPECIFIC AREAS OF DATA PROCESSING SYSTEMS

Persons entitled to use the data processing system are only able to access Personal Data within the scope and to the extent covered by their respective access permission (authorization), and that Personal Data cannot be read, copied, modified or removed without authorization.

- Employee policies and training with respect to each employee's access rights to Personal Data.
- PatSnap users have unique login credentials and role-based access control are used to restrict access to particular functions.
- Effective and measured disciplinary action against individuals who access Personal Data without authorization.

- Controlling access to account data and customer Personal Data via role-based access controls (RBAC) in compliance with the security principle of “least privilege”.
- Internal segmentation and logical isolation of PatSnap's employees to enforce least privilege access policies.
- Authorization of access rights by system owner as well as monitoring and logging.
- Ongoing review of accounts and privileges (typically every 2-4 months depending on the particular system and sensitivity of data to which it provides access).
- Controlled and documented destruction of data.
- Developers have access to fictitious test data.

3. AVAILABILITY CONTROL

PatSnap has implemented suitable measures to ensure that Personal Data is protected from accidental destruction or loss.

- Global and redundant service infrastructure that is set up with full disaster recovery sites.
- Constantly evaluating data centers and Internet Service Providers (ISPs) to optimize performance for its customers in regards to bandwidth, latency and disaster recovery isolation.
- Situating data centers in secure co-location facilities that are ISP carrier-neutral and provide physical security, redundant power and infrastructure redundancy.
- Service level agreements from data center providers and ISPs to ensure high levels of availability.
- PatSnap maintains full capacity disaster recovery (DR) sites and annually tests its DR plan.

4. TRANSMISSION CONTROL

PatSnap has implemented suitable measures to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media.

- Use of adequate firewall and encryption technologies to protect the gateways and pipelines through which the data travels.

- Sensitive Personal Data is encrypted during transmission using up-to-date versions of TLS and/or other security protocols (HTTPS) using strong encryption algorithms and keys.
- End-to-end encryption of screen sharing for remote access, support and real-time communication.
- Use of integrity checks to monitor the completeness and correctness of the transfer of data (e.g. SFTP).

5. INPUT CONTROL

PatSnap has implemented suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data have been input into data processing systems or removed.

- Authentication of the authorized personnel.
- Segregation and protection of all stored Personal Data via database schemas, logical access controls and/or encryption.
- Utilization of user identification credentials.
- Physical security of data processing facilities.
- Session time outs.

6. SEPERATION OF PROCESSING FOR DIFFERENT PURPOSES

PatSnap has implemented suitable measures to ensure that Personal Data collected for different purposes can be processed separately. Personal data are permitted to be used only for the purpose for which they were originally collected.

7. DOCUMENTATION

PatSnap keeps documentation of technical and organizational measures in case of audits and for the conservation of evidence. PatSnap takes reasonable steps to ensure that persons employed by it and other persons at the place of work are aware of and comply with the technical and organizational measures set forth in this document. PatSnap, at its election, may make non-confidential portions of audit reports available to customers to verify compliance with the technical and organizational measures undertaken in this document.

8. MONITORING

PatSnap does not access Customer Personal Data, except to provide services to the Customer which PatSnap is obligated to perform in support of the Customer experience

as required by law, or on request by Customer. PatSnap has implemented suitable measures to monitor access restrictions of PatSnap's system administrators and to ensure that they act in accordance with instructions received.

This is accomplished by:

- Individual appointment of system administrators.
- Adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for a reasonable period of time.
- Regular audits of system administrators' activity to assess compliance with assigned tasks.

9. DEFINITIONS

"PatSnap" means Patsnap (UK) Ltd and all of its direct and indirect subsidiaries.

"Customer" means any purchaser of any PatSnap offering.

"Personal Data" means any information directly or indirectly relating to any identified or identifiable natural person.

"Security Framework" refers to the collection of PatSnap's policies and procedures governing information security, including, but not limited to, policies, trainings, education, monitoring, investigation and enforcement of its data management and security efforts.