CELOXIS DATA PROCESSING ADDENDUM

Last updated on August 17, 2023

BY CLICKING ON THE "I AGREE" (OR SIMILAR BUTTON) FOR ACCEPTANCE OF THE EULA AGREEMENT OR USING THE SOFTWARE AND THE SERVICES, YOU INDICATE YOUR ASSENT TO THE FOLLOWING TERMS OF THIS DATA PROCESSING ADDENDUM.

This Data Processing Addendum ("**Addendum**") forms part of the End User License Agreement – On-premise or SaaS as the case may be ("**Agreement**") between: (i) You (defined below) acting on your own behalf of our Client opted for the Services and as agent for each of Your Authorized Affiliate); and (ii) Celoxis acting on its own behalf and as agent for each Celoxis Affiliate.

All capitalized terms not defined herein shall have the meaning set forth in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall form an integral part of the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. Definitions

In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

“**Authorized Affiliate**” means any of Your Affiliate(s) who (a) are subject to the data protection laws and regulations of the European Union, the European Economic Area and/ or their Member States, and/or the United Kingdom and (b) are permitted to use the Services/ Software pursuant to the Agreement between You and Celoxis.

“**Celoxis Affiliate**” means any of the Celoxis Group companies (as defined below).

“**Celoxis Group**” means “**We**” “**Us**”, “**Celoxis**” and its subsidiaries or affiliates of Celoxis engaged in the Processing of Personal Data.

“**You**” means any client of Celoxis incorporated and based out of the E.U. territory who has opted for the Services of Celoxis and have opened a User Account with Celoxis for the benefit of its Users including their Authorised Affiliates.

“**Your Personal Data**” means Personal Data included in the “**Member Data**” or “**Data**” (as such terms are defined in the Agreement).

“**Data Protection Laws and Regulations**” means all laws and regulations, including laws and regulations of the European Union and their Member States, and the UK Data Protection Laws applicable to the Processing of Personal Data under the Agreement.

"**Data Transfer**" means (1) a transfer of Personal Data from you or any of your Authorized Affiliate to a Celoxis Group member or a Sub-processor; or (2) an onward transfer of Personal Data from a Celoxis

Group member to a Sub-processor, or between two establishments of a Sub-processor, in each case, where such transfer originates from the European Union, to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**EU Standard Contractual Clauses**" means the contractual clauses attached hereto as Schedule 1 pursuant to the European Commission's IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection (or any updated version thereof).

"IDTA" means International Data Transfer Addendum to the EU Standard Contractual Clauses the contractual clauses attached hereto as Schedule 2 issued by the commissioner under S119A(1) Data Protection Act 2018.

"**Sub-processor**" means any Processor engaged by Celoxis or a member of the Celoxis Group and that Processes Your Personal Data.

"**Security Specifications**" means the Security and Architecture information applicable to the Services purchased by you, available at: https://www.celoxis.com/security as updated from time to time by Celoxis.

"**UK Data Protection Laws"** means the UK GDPR, the United Kingdom Data Protection Act 2018, the Privacy and Electronic Communications Regulations, and any regulation superseding any of the foregoing.

1.2 The terms, "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**" and "**Supervisory Authority**" shall have the same meaning as in the Data Protection Laws and Regulations.

2. Processing of Your Personal Data

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, You are the Controller, Celoxis is the Processor and that Celoxis or its Affiliates will engage Sub-processors pursuant to the requirements set forth in Section 5 "Subprocessing" below.

2.2 Your Processing of Personal Data. You shall, in your use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Your instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. You shall have sole responsibility for the accuracy, quality, and legality of Personal Data, and the means by which You acquired Personal Data.

2.3 Celoxis's Processing of Personal Data. Celoxis shall treat Personal Data as confidential information and shall only Process Personal Data on behalf of and in accordance with your documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by you (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.4 Details of the Processing. The subject-matter of Processing of Personal Data by Celoxis is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the categories of Data Subjects and types of Personal Data Processed under this Addendum are further specified in Annex A (Details of the Processing) to this Addendum, as required by article 28(3) of the GDPR. Nothing in Annex A confers any right or imposes any obligation on any party to this Addendum.

3. Celoxis and Celoxis Affiliate Personnel

Celoxis and each Celoxis Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Celoxis Group member who has access to Your Personal Data, ensuring in each case that access is limited to those individuals as necessary for the provision of Services under the Agreement, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Controls for the Protection of your Data. Celoxis shall maintain reasonable technical and organizational measures for protection of the security, confidentiality and integrity of your Data, as set forth in the Security Specifications.

4.2 Appropriateness of security measures. You acknowledge that You have assessed the security measures implemented by Celoxis, that You consider those measures to be appropriate taking into account the risk of likelihood and severity for the rights and freedoms of Data Subjects resulting from the Processing of Your Personal Data and, as between the parties and the Data Subjects and Supervisory Authorities, You are solely responsible for such determination of appropriateness.

5. Subprocessing

5.1 Appointment of Sub-processors. You acknowledge and agree that (a) Celoxis’s Affiliates may be retained as Sub-processors; and (b) Celoxis and Celoxis’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services.

6. Data Subject Rights

6.1 Notification. Celoxis shall, to the extent legally permitted, notify You if Celoxis receives a request from a Data Subject to exercise the Data Subject's rights of access, rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, objection to the Processing, as well as its right not to be subject to an automated individual decision making (“Data Subject Request”).

6.2 Assistance. Taking into account the nature of the Processing, Celoxis shall assist You by appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfilment of your obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent You, in your use of the Services, do not have the ability to address a Data Subject Request, Celoxis shall upon your request provide commercially reasonable efforts to assist You in responding to such Data Subject Request, to the extent Celoxis is legally permitted to do so and if the response to such

Data Subject Request is required under Data Protection Laws and Regulations. You shall be responsible for any costs arising from Celoxis's provision of any such assistance.

7. Personal Data Breach

7.1 Celoxis shall notify You, upon Celoxis coming across any Personal Data Breach or any Sub-processor notifying us of a Personal Data Breach affecting Your Personal Data by providing You with available information to help you meet your obligations under the Data Protection Laws and Regulations to report or inform Data Subjects of the Personal Data Breach.

7.2 To the extent the Personal Data Breach is proved by You to be attributable to Celoxis, Celoxis shall co-operate with You and take such reasonable commercial steps as are directed by You to assist in the investigation, mitigation and remediation of each such Personal Data Breach, to the extent the remediation is within Celoxis's reasonable control. The obligations herein shall not apply to incidents that are caused by you or your Users.

8. Data Protection Impact Assessment and Prior Consultation

Upon your request, Celoxis shall provide you with reasonable cooperation and assistance needed to fulfil your obligation under the GDPR and or UK GDPR as the case may be to carry out a data protection impact assessment related to your use of the Services, to the extent you do not otherwise have access to the relevant information, and to the extent such information is available to Celoxis.

Celoxis shall provide reasonable assistance to You with respect to the cooperation or prior consultation with the Supervisory Authority in the performance of your tasks relating to a data protection impact assessment. You shall be responsible for any costs arising from Celoxis's provision of such assistance.

9. Return and Deletion of Your Personal Data

9.1 Any time before cessation of any Services (which also involves the Processing of Your Personal Data by Celoxis) or deletion of your account by you (the "Cessation Date"), you can download all of your Personal Data in the then current format in which it was stored.

9.2 After the Cessation Date, Celoxis will as per the then prevailing policies of Celoxis, delete and procure the deletion of all copies of Your Personal Data Processed by Celoxis and any Sub-processor to the extent allowed by applicable law.

10. Audit rights

10.1 Upon your written request and at your sole cost, Celoxis shall within a reasonable period of time and at our convenience make available to you (or your independent, third-party auditor that is not a competitor of Celoxis) information regarding Celoxis's compliance with the obligations set forth in this Addendum in the form of the third-party certifications and audits set forth in the Security Specifications in the conditions set forth in Section 4.2 and to the extent Celoxis makes them generally available to our customers. You acknowledge that a flat rate of USD 10000 per day shall apply for any audit undertaken by you or your independent, third-party auditors.

10.2 You may request an on-site audit of the procedures relevant to the protection of Personal Data. You shall reimburse Celoxis for any time expended for any such on-site audit at the Celoxis's then-current professional services rates in addition to the flat per day rate of USD 10000, which shall be made available to you upon request. Before the commencement of any such on-site audit, you and Celoxis shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which you shall be responsible. You shall promptly notify Celoxis with information regarding any non-compliance discovered during the course of an audit.

10.3 You may only mandate an auditor for the purposes of section 10, if the auditor is mutually approved by agreement between the parties in writing from time to time.

10.4 In any case, when undertaking an audit, You shall (and ensure that each of your mandated auditors) avoid causing damage, injury or disruption to the Celoxis Group member premises, equipment, personnel and business while conducting an audit or inspection.

11. Mechanism for Data Transfers

11.1 Standard Contractual Clauses. The EU Standard Contractual Clauses and the UK IDTA and the additional terms specified in this Section 11 apply to the legal entity that has executed the required EU Standard Contractual Clauses and the UK IDTA as a data exporter and its Authorized Affiliates. For the purpose of the EU Standard Contractual Clauses and the UK IDTA and this Section 11, the aforementioned entities shall be deemed “data exporters”.

11.2 Instructions. This Addendum and the Agreement are your complete and final documented instructions at the time of signature of the Agreement to Celoxis for the Processing of Personal Data. Instructions by you to Process Personal Data are described in Section 2.3 of this Addendum.

11.3 Sub-processors. You acknowledge and expressly agree that Celoxis may use and/or engage Sub-processors as described in Section 5 of this Addendum.

12. General Terms

Governing law and jurisdiction

12.1 Without prejudice to the clauses in relation to Jurisdiction and Governing Law of the EU Standard Contractual Clauses and the UK IDTA :

12.1.1 .the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

12.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

Order of precedence and severance

12.2 In the event of any conflict or inconsistency between this Addendum and the applicable EU Standard Contractual Clauses and the UK IDTA, the applicable EU Standard Contractual Clauses and the UK IDTA shall prevail. With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

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

List of Annexes

Annex A: Details of Processing of Personal Data

Schedule 1: EU Standard Contractual Clauses

Schedule 2: UK IDTA

ANNEX A: DETAILS OF PROCESSING OF PERSONAL DATA

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

Subject matter, Nature and Purpose of Processing

Celoxis will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the allied documentation as may be agreed in writing by the parties, and as further instructed by you in your use of the Services.

Your Obligations and rights

The obligations and rights provided to you are set out in the Agreement and this Addendum.

Duration of Processing

Subject to Section 9 of this Addendum, Celoxis will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing. Further, Celoxis may Process Personal Data for the purpose of sharing with you any future updates / upgrades about its services, offerings or solution etc, after expiry or termination of the Agreement.

Categories of Data Subjects

You may submit Personal Data to the Services, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

The employees (Users) or your authorized personnel who are beneficiary of the Services (under the Agreement).

Type of Personal Data

You may submit Personal Data to the Services, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to the following categories of Personal Data:

Official Contact Information of the Users i.e. your employees, or any other personnel authorized by you.

SCHEDULE 1: EU 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)

(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

(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, 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.

(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)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

(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 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.

ANNEX I

Data exporter(s):

1.Name: *The entity identified as customer in the Agreement.*

Address: *The address for customer specified in the Agreement.*

Contact person's name, position and contact details: *The contact details associated with Customer's account, or as otherwise specified in the Agreement.*

Activities relevant to the data transferred under these Clauses:

Signature and date: *By using the Services to transfer Personal Data to Third Countries, the data exporter will be deemed to have signed this Annex I*

Role (controller/processor)*: Controller*

2 Data importer(s):

1.Name: Celoxis Technologies Pvt. Ltd.

Address: *3 Shreyas Eterna, NDA Pashan Road, Bavdhan, Pune-411021*

Contact person's name, position and contact details: e-mail: privacy@celoxis.com

Activities relevant to the data transferred under these Clauses: *Celoxis will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the allied documentation as may be agreed in writing by the parties, and as further instructed by you in your use of the Services*

Signature and date: *By transferring Personal Data to third countries on Data Exporter's instructions, the data importer will be deemed to have signed this Annex*

Role (controller/processor): Processor.

B. ***DESCRIPTION OF TRANSFER***

Categories of data subjects whose personal data is transferred: *Data exporter may submit Personal Data to Celoxis, to the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:*

The employees (Users) or your authorized personnel who are beneficiary of the Services (under the Agreement).

Categories of personal data transferred: *Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:*

Official Contact Information of the Users i.e. your employees, or any other personnel authorized by you.

Logs for use of Services.

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.

Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis). *As required for the performance of Services.*

Nature of the processing: *The personal data transferred will be subject to the following basic processing activities:*

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing: *The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to 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: *We will retain your Personal Information for as long as required, for providing the Services. We may also retain and use your Personal Information as long as is required in order to comply with our legal obligations, resolve disputes, and enforce our agreements.*

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

The Data Protection Commission – Ireland

ANNEX II

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

Celoxis Cloud Security & Infrastructure

ANNEX III

LIST OF SUB-PROCESSORS

Name	Purpose
Amazon Web Services (AWS)	Cloud computing services
Google Cloud	Cloud computing services
Zendesk	Cloud-based helpdesk software
Freshsales	Cloud-based CRM software
Google Workspaces	Office email service
SendGrid	Email delivery service
Hubspot	Cloud-based CRM software
Freshmarketer	Cloud-based marketing software

Schedule 2: UK IDTA

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: *As per Schedule 1, Annex I of this DPA.* Trading name (if different): Main address (if a company registered address): *As per Schedule 1 , Annex I of this DPA.* Official registration number (if any) (company number or similar identifier):	Full legal name: *As per Schedule 1, Annex I of this DPA*. Trading name (if different): Main address (if a company registered address): *As per Schedule 1 , Annex I of this DPA.* Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): *As per Schedule 1 , Annex I of this DPA.* Job Title: *As per Schedule 1 , Annex I of this DPA.* Contact details including email: *As per Schedule 1 , Annex I of this DPA.*	Full Name (optional): *As per Schedule 1 , Annex I of this DPA.* Job Title: *As per Schedule 1 , Annex I of this DPA.* Contact details including email: *As per Schedule 1 , Annex I of this DPA.*
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ **The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information**: Date: As per the DPA date. Reference (if any):

	Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	NA	NA	NA	NA	NA	NA
2	NA	NA	NA	NA	NA	NA
3	NA	NA	NA	NA	NA	NA
4	NA	NA	NA	NA	NA	NA

Table 3: Appendix Information

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:
Annex 1B: Description of Transfer:
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:
Annex III: List of Sub processors (Modules 2 and 3 only):

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ **Importer** ☒ **Exporter** ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance

	with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.