NISOS

# NISOS HOLDINGS INC.
# DATA PROCESSING ADDENDUM

**THIS DATA PROCESSING ADDENDUM** ("**DPA**") is entered into as of the Addendum Effective Date by and between: (1) **NISOS HOLDINGS INC.**, whose details are set out in the Order Form ("**Nisos**"); and (2) the entity or other person who is a counterparty to the Order Form ("**Client**"), together the "**Parties**" and each a "**Party**", and forms a valid and binding part of the Order Form.

## 1. INTERPRETATION

1.1 In this DPA the following terms shall have the meanings set out in this Section 1, unless expressly stated otherwise:

(a) "**Addendum Effective Date**" means the date both Parties have signed the Order Form.

(b) "**Applicable Data Protection Laws**" means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Client Personal Data under the Terms, including, without limitation, the GDPR (as and where applicable).

(c) "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(d) "**Client Personal Data**" means any Personal Data Processed by Nisos or its Sub-Processor on behalf of Client to perform the Services under the Order Form.

(e) "**Data Subject Request**" means the exercise by a Data Subject of its rights in accordance with Applicable Data Protection Laws in respect of Client Personal Data and the Processing thereof.

(f) "**Data Subject**" means the identified or identifiable natural person to whom Client Personal Data relates.

(g) "**Data Transfer Mechanism**" means in respect of: (i) any EU Restricted Transfer, the EU SCCs; and (ii) any UK Restricted Transfer, the UK Addendum.

(h) "**EEA**" means the European Economic Area.

(i) "**EU SCCs**" means the standard contractual clauses approved by the European Commission pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 applicable to an EU Restricted Transfer (as determined in accordance with Paragraph 6.2 of Annex 1 (European Annex)), as set out in Attachment 2 of Annex 1 (European Annex). References to "**Modules**" shall refer to modules of the EU SCCs.

(j) "**GDPR**" means, as and where applicable to Processing concerned: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"); and/or (ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended, including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("**UK GDPR**"), including, in each case (i) and (ii) any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or re-enactment, to or of the foregoing. References to "**Articles**" and "**Chapters**" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

(k) "**Mandatory Clauses**" means the mandatory clauses of the UK Addendum, as shown in Part Four of the document presently published at https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf.

(l) "**Nisos' Privacy Notice**" means Nisos' privacy notice as made available at https://www.nisos.com/privacy-policy/, as updated from time to time.

(m) **"Order Form"** means the order form entered into by Nisos and the Client, comprising the order form, the Terms, and this DPA.

(n) "**Personal Data Breach**" means a breach of Nisos' security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Client Personal Data in Nisos' possession, custody or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Client Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

(o) "**Personal Data**" means "personal data," "personal information," "personally identifiable information" or similar term defined in Applicable Data Protection Laws.

(p) "**Personnel**" means a person's employees, agents, consultants or contractors.

(q) "**Process**" and inflection thereof means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(r) "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

(s) "**Restricted Data**" has the meaning given to it in Section 8.4.

(t) "**Restricted Transfer**" means the disclosure, grant of access or other transfer of Client Personal Data to any person located in: (i) in the context of the EEA, any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission (an "**EU Restricted Transfer**"); and (ii) in the context of the UK, any country or territory outside the UK, which does not benefit from an adequacy decision from the UK Government (a "**UK Restricted Transfer**"), which would be prohibited without a legal basis under Chapter V of the GDPR.

(u) "**Service Data**" means any data relating to the use, support and/or operation of the Services, which is collected directly by Nisos from and/or about users of the Services and/or Client's use of the Service for use for its own purposes (certain of which may constitute Personal Data).

(v) "**Services**" means those services and activities to be supplied to or carried out by or on behalf of Nisos for Client pursuant to the Order Form.

(w) "**Sub-Processor**" means any third party appointed by or on behalf of Nisos to Process Client Personal Data.

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

(y) **"Terms"** means the terms and conditions entered into by and between the Parties pursuant to the Order Form and into which this DPA is incorporated.

(z) "**UK Addendum**" means the template addendum B1.0 issued by the ICO under s119A(1) of the Data Protection Act 2018, in force from 21 March 2022, as set out in Attachment 3 of Annex 1 (European Annex).

In this DPA, unless otherwise defined in this DPA, all capitalised terms shall have the meaning given to them in the Terms.

## 2. SCOPE OF THIS DATA PROCESSING ADDENDUM

2.1 The front-end of this DPA applies generally to Nisos' Processing of Client Personal Data under the Order Form.

2.2 Annex 1 (European Annex) to this DPA applies only if and to the extent Nisos' Processing of Client Personal Data under the Order Form is subject to the GDPR.

## 3. PROCESSING OF CLIENT PERSONAL DATA

*Nisos as a Processor*

3.1 Subject to Sections 3.3 to Section 3.5, Nisos shall not Process Client Personal Data other than on Client's instructions or as required by applicable laws.

3.2 Client instructs Nisos to Process Client Personal Data as necessary to provide the Services to Client under and in accordance with the Order Form and the Terms.

*Nisos as a Controller*

3.3 Client acknowledges that Nisos may Process Service Data for its own purposes, such as:

(a) for accounting, tax, billing, audit, and compliance purposes;

(b) to provide, improve, develop, optimise and maintain the Services;

(c) to investigate fraud, spam, wrongful or unlawful use of the Services;

(d) to create, and derive from Processing under this DPA, deidentified, anonymised and/or aggregated data that does not identify Client or any Data Subject; and/or

(e) as otherwise permitted or required by applicable law.

3.4 In respect of any such Processing described in Section 3.3, Nisos:

(a) acts as an independent Controller;

(b) shall comply with Applicable Data Protection Laws (if and as applicable in the context);

(c) shall Process such Service Data as described in Nisos' Privacy Notice; and

(d) where possible, shall apply technical and organisational safeguards to any relevant Personal Data that are no less protective than the Security Measures.

3.5 In respect of its Processing of Client Personal Data, Client agrees to comply with Applicable Data Protection Laws (if and as applicable in the context), including in relation to the collection and disclosure of Client Personal Data.

## 4. NISOS PERSONNEL

Nisos shall take commercially reasonable steps to ascertain the reliability of any Nisos Personnel who Process Client Personal Data, and shall enter into written confidentiality agreements with all Nisos Personnel who Process Client Personal Data that are not subject to professional or statutory obligations of confidentiality.

## 5. SECURITY

5.1 Nisos shall implement and maintain technical and organisational measures in relation to Client Personal Data designed to protect Client Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access as described in Annex 2 (Security Measures) (the "**Security Measures**").

5.2 Nisos may update the Security Measures from time to time, provided the updated measures do not materially decrease the overall protection of Client Personal Data.

## 6. DATA SUBJECT RIGHTS

6.1 Nisos, taking into account the nature of the Processing of Client Personal Data, shall provide Client with such assistance as may be reasonably necessary and technically feasible to assist Client in fulfilling its obligations to respond to Data Subject Requests. If Nisos receives a Data Subject Request, Client will be responsible for responding to any such request.

6.2 Nisos shall:

(a) promptly notify Client if it receives a Data Subject Request; and

(b) not respond to any Data Subject Request, other than to advise the Data Subject to submit the request to Client, except on the written instructions of Client or as required by Applicable Data Protection Laws.

6.3 Operational clarifications:

(a) When complying with its transparency obligations under Clause 8.3 of the EU SCCs, Client agrees that it shall not provide or otherwise make available, and shall take all appropriate steps to protect, Nisos' and its licensors' trade secrets, business secrets, confidential information and/or other commercially sensitive information.

(b) For the purposes of Clause 15.1(a) of the EU SCCs, except to the extent prohibited by applicable law and/or the relevant public authority, as between the Parties, Client agrees that it shall be solely responsible for making any notifications to relevant Data Subject(s) if and as required.

(c) Except to the extent prohibited by applicable law, Client shall be fully responsible for all time spent by Nisos (at Nisos' then-current professional services rates) in Nisos' cooperation and assistance provided to Client under this Section 6, and shall on demand reimburse Nisos any such costs incurred by Nisos.

## 7. PERSONAL DATA BREACH

*Breach notification and assistance*

7.1 Nisos shall notify Client without undue delay upon Nisos' discovering a Personal Data Breach affecting Client Personal Data. Nisos shall provide Client with information (insofar as such information is within Nisos' possession and knowledge and does not otherwise compromise the security of any Personal Data Processed by Nisos) to allow Client to meet its obligations under the Applicable Data Protection Laws to report the Personal Data Breach. Nisos' notification of or response to a Personal Data Breach shall not be construed as Nisos' acknowledgement of any fault or liability with respect to the Personal Data Breach.

7.2 Nisos shall reasonably co-operate with Client and take such commercially reasonable steps as may be directed by Client to assist in the investigation of any such Personal Data Breach.

7.3 Client is solely responsible for complying with notification laws applicable to Client and fulfilling any third-party notification obligations related to any Personal Data Breaches.

7.4 Operational clarifications:

(a) Except to the extent prohibited by applicable law, Client shall be fully responsible for all time spent by Nisos (at Nisos' then-current professional services rates) in Nisos' cooperation and assistance provided to Client under Section 7.2, and shall on demand reimburse Nisos any such costs incurred by Nisos.

*Notification to Nisos*

7.5 If Client determines that a Personal Data Breach must be notified to any Supervisory Authority, any Data Subject(s), the public or others under Applicable Data Protection Laws, to the extent such notice directly or indirectly refers to or identifies Nisos, where permitted by applicable laws, Client agrees to:

(a) notify Nisos in advance; and

(b) in good faith, consult with Nisos and consider any clarifications or corrections Nisos may reasonably recommend or request to any such notification, which: (i) relate to Nisos' involvement in or relevance to such Personal Data Breach; and (ii) are consistent with applicable laws.

## 8. CLIENT'S RESPONSIBILITIES

8.1 Client agrees that, without limiting Nisos' obligations under Section 5 (Security), Client is solely responsible for its use of the Services, including (a) making appropriate use of the Services to maintain a level of security appropriate to the risk in respect of the Client Personal Data; (b) securing the account authentication credentials, systems and devices Client uses to access the Services; (c) securing Client's systems and devices that Nisos uses to provide the Services; and (d) backing up Client Personal Data.

8.2 Client shall ensure:

(a) that there is, and will be throughout the term of the Order Form, a valid legal basis for the Processing by Nisos of Client Personal Data in accordance with this DPA and the Terms (including, any and all instructions issued by Client from time to time in respect of such Processing) for the purposes of all Applicable Data Protection Laws (including Article 6, Article 9(2) and/or Article 10 of the GDPR (where applicable)); and

(b) that all Data Subjects have (i) been presented with all required notices and statements (including as required by Article 12-14 of the GDPR (where applicable)); and (ii) provided all required consents, in each case (i) and (ii) relating to the Processing by Nisos of Client Personal Data.

8.3 Client agrees that the Service, the Security Measures, and Nisos' commitments under this DPA are adequate to meet Client's needs, including with respect to any security obligations of Client under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Client Personal Data.

8.4 Except as expressly otherwise agreed in the Order From, Client shall not provide or otherwise make available to Nisos any Client Personal Data that contains any (a) Social Security numbers or other government-issued identification numbers; (b) protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (c) health insurance information; (d) biometric information; (e) passwords to any online accounts; (f) credentials to any financial accounts; (g) tax return data; (h) any payment card information subject to the Payment Card Industry Data Security Standard; (i) Personal Data of children under 13 years of age; or (j) any other information that falls within any special categories of personal data (as defined in GDPR) and/or data relating to criminal convictions and offences or related security measures (together, "**Restricted Data**"). Where Client provides Restricted Data to Nisos, or otherwise makes Restricted Data available, Client warrants and represents that it is permitted to do so under Applicable Data Protection Laws, including in relation to the collection and disclosure of such Restricted Data.

## 9. LIABILITY

The total aggregate liability of either Party towards the other Party, howsoever arising, under or in connection with this DPA and the Data Transfer Mechanism(s) (if and as they apply) will under no circumstances exceed any limitations or caps on, and shall be subject to any exclusions of, liability and loss agreed by the Parties in the Terms; **provided that**, nothing in this Section 9 will affect any person's liability to Data Subjects under the third-party beneficiary provisions of the Data Transfer Mechanism(s) (if and as they apply).

## 10. INCORPORATION AND PRECEDENCE

10.1 This DPA shall be incorporated into and form part of the Terms with effect from the Addendum Effective Date.

10.2 In the event of any conflict or inconsistency between:

(a) this DPA and the Terms and/or the Order Form, this DPA shall prevail; or

(b) any Data Transfer Mechanism(s) entered into pursuant to Paragraph 6 of Annex 1 (European Annex) and this DPA, the Terms, and/or the Order Form, the Data Transfer Mechanism(s) shall prevail in respect of the Restricted Transfer to which they apply.

## Annex 1

## European Annex

1. **PROCESSING OF CLIENT PERSONAL DATA**

1.1 The Parties acknowledge and agree that the details of Nisos' Processing of Personal Data under this DPA and the Order Form (including the respective roles of the Parties relating to such Processing) are as set out in Attachment 1 of Annex 1 (European Annex) to the DPA.

1.2 Where Nisos receives an instruction from Client that, in its reasonable opinion, infringes the GDPR, Nisos shall inform Client.

1.3 Client acknowledges and agrees that any instructions issued by Client with regards to the Processing of Client Personal Data by or on behalf of Nisos pursuant to or in connection with the Order Form shall be in strict compliance with the GDPR and all other applicable laws.

2. **SUBPROCESSING**

2.1 Client generally authorises Nisos to appoint Sub-Processors in accordance with this Paragraph 2.

2.2 Nisos may continue to use those Sub-Processors already engaged by Nisos as at the date of this DPA (as those Sub-Processors are shown, together with their respective functions and locations, in Annex 3 (Authorised Sub-Processors) (the "**Sub-Processor List**").

2.3 Nisos shall give Client prior written notice of the appointment of any proposed Sub-Processor, including reasonable details of the Processing to be undertaken by the Sub-Processor, by providing Client with an updated copy of the Sub-Processor List via a 'mailshot' or similar bulk distribution mechanism sent via email to Client's contact point as set out in Attachment 1 of Annex 1 (European Annex). If, within fourteen (14) days of receipt of that notice, Client notifies Nisos in writing of any objections (on reasonable grounds) to the proposed appointment:

(a) Nisos shall use reasonable efforts to make available a commercially reasonable change in the provision of the Services, which avoids the use of that proposed Sub-Processor; and

(b) where: (i) such a change cannot be made within fourteen (14) days from Nisos' receipt of Client's notice; (ii) no commercially reasonable change is available; and/or (iii) Client declines to bear the cost of the proposed change, then either Party may by written notice to the other Party with immediate effect terminate the Order Form, either in whole or to the extent that it relates to the Services which require the use of the proposed Sub-Processor, as its sole and exclusive remedy.

2.4 If Client does not object to Nisos' appointment of a Sub-Processor during the objection period referred to in Paragraph 2.3, Client shall be deemed to have approved the engagement and ongoing use of that Sub-Processor.

2.5 With respect to each Sub-Processor, Nisos shall maintain a written contract between Nisos and the Sub-Processor that includes terms which offer at least an equivalent level of protection for Client Personal Data as those set out in this DPA (including the Security Measures). Nisos shall remain liable for any breach of this DPA caused by a Sub-Processor.

2.6 Operational clarifications:

(a) The terms and conditions of this Paragraph 2 apply in relation to Nisos' appointment and use of Sub-Processors under the Data Transfer Mechanism(s).

(b) Any approval by Client of Nisos' appointment of a Sub-Processor that is given expressly or deemed given pursuant to this Paragraph 2 constitutes Client's documented instructions to effect disclosures and onward transfers to any relevant Sub-Processors if and as required under Clause 8.8 of the EU SCCs.

## 3. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

3.1 Nisos, taking into account the nature of the Processing and the information available to Nisos, shall provide reasonable assistance to Client, at Client's cost, with any data protection impact assessments and prior consultations with Supervisory Authorities which Client reasonably considers to be required of it by Article 35 or Article 36 of the GDPR, in each case solely in relation to Processing of Client Personal Data by Nisos.

3.2 Operational clarification: Except to the extent prohibited by applicable law, Client shall be fully responsible for all time spent by Nisos (at Nisos' then-current professional services rates) in Nisos' provision of any cooperation and assistance provided to Client under Paragraph 3.1, and shall on demand reimburse Nisos any such costs incurred by Nisos.

## 4. RETURN AND DELETION

4.1 Subject to Paragraph 4.2 and 4.3, upon the date of cessation of any Services involving the Processing of Client Personal Data (the "**Cessation Date**"), Nisos shall promptly cease all Processing of Client Personal Data for any purpose other than for storage or as otherwise permitted or required under this DPA.

4.2 Subject to Paragraph 4.4, to the extent technically possible in the circumstances (as determined in Nisos' sole discretion), on written request to Nisos (to be made no later than fourteen (14) days after the Cessation Date ("**Post-cessation Storage Period**")), Nisos shall within fourteen (14) days of such request:

(a) return a complete copy of all Client Personal Data within Nisos' possession to Client by secure file transfer, promptly following which Nisos shall delete or irreversibly anonymise all other copies of such Client Personal Data; or

(b) either (at its option) delete or irreversibly anonymise all Client Personal Data within Nisos' possession.

4.3 In the event that during the Post-cessation Storage Period, Client does not instruct Nisos in writing to either delete or return Client Personal Data pursuant to Paragraph 4.2, Nisos shall promptly after the expiry of the Post-cessation Storage Period either (at its option) delete; or irreversibly render anonymous, all Client Personal Data then within Nisos possession to the fullest extent technically possible in the circumstances.

4.4 Nisos may retain Client Personal Data where permitted or required by applicable law, for such period as may be required by such applicable law, provided that Nisos shall:

(a) maintain the confidentiality of all such Client Personal Data; and

(b) Process the Client Personal Data only as necessary for the purpose(s) specified in the applicable law permitting or requiring such retention.

4.5 Operational clarification: Certification of deletion of Client Personal Data as described in Clauses 8.5 and 16(d) of the EU SCCs shall be provided only upon Client's written request.

## 5. AUDIT RIGHTS

5.1 Nisos shall make available to Client on request, such information as Nisos (acting reasonably) considers appropriate in the circumstances to demonstrate its compliance with this DPA.

5.2 Subject to Paragraphs 5.3 to 5.8, in the event that Client (acting reasonably) is able to provide documentary evidence that the information made available by Nisos pursuant to Paragraph 5.1 is not sufficient in the circumstances to demonstrate Nisos' compliance with this DPA, Nisos shall allow for and contribute to audits, including on-premise inspections, by Client or an auditor mandated by Client in relation to the Processing of Client Personal Data by Nisos.

5.3 Client shall give Nisos reasonable notice of any audit or inspection to be conducted under Paragraph 5.2 (which shall in no event be less than fourteen (14) days' notice) and shall use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing any destruction, damage, injury or disruption to Nisos' premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of Nisos' other clients or the availability of Nisos' services to such other clients).

5.4 Prior to conducting any audit, Client must submit a detailed proposed audit plan providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Nisos will review the proposed audit plan and provide Client with any concerns or questions (for example, any request for information that could compromise Nisos security, privacy, employment or other relevant policies). Nisos will work cooperatively with Client to agree on a final audit plan.

5.5 If the controls or measures to be assessed in the requested audit are addressed in a SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Client's audit request ("**Audit Report**") and Nisos has confirmed in writing that there are no known material changes in the controls audited and covered by such Audit Report(s), Client agrees to accept provision of such Audit Report(s) in lieu of requesting an audit of such controls or measures.

5.6 Nisos need not give access to its premises for the purposes of such an audit or inspection:

(a) where an Audit Report is accepted in lieu of such controls or measures in accordance with Paragraph 5.5;

(b) to any individual unless they produce reasonable evidence of their identity;

(c) to any auditor whom Nisos has not approved in advance (acting reasonably);

(d) to any individual who has not entered into a non-disclosure agreement with Nisos on terms acceptable to Nisos;

(e) outside normal business hours at those premises; or

(f) on more than one occasion in any calendar year during the term of the Order Form, except for any audits or inspections which Client is required to carry out under the GDPR or by a Supervisory Authority.

5.7 Nothing in this DPA shall require Nisos to furnish more information about its Sub-Processors in connection with such audits than such Sub-Processors make generally available to their customers.

5.8 <u>Operational clarifications</u>:

(a) Except to the extent prohibited by applicable law, Client shall be fully responsible for all time spent by Nisos (at Nisos' then-current professional services rates) in Nisos' provision of any cooperation and assistance provided to Client under this Paragraph 5 (excluding any costs incurred in the procurement, preparation or delivery of Audit Reports to Client pursuant to Paragraph 5.5), and shall on demand reimburse Nisos any such costs incurred by Nisos.

(b) The audits described in Clauses 8.9(c) and 8.9(d) of the EU SCCs shall be subject to any relevant terms and conditions detailed in this Paragraph 5.

6. **RESTRICTED TRANSFERS**

6.1 The Parties acknowledge that Client's transmission of Client Personal Data to Nisos hereunder may involve a Restricted Transfer. The relevant Data Transfer Mechanism(s) that may be entered into under Paragraph 6.2 and/or 6.3 shall apply and have effect only if and to the extent permitted and required under the EU GDPR and/or UK GDPR (if and as applicable) to establish a valid basis under Chapter V of the EU GDPR and/or UK GDPR in respect of the transfer from Client to Nisos of Client Personal Data.

*EU Restricted Transfers*

6.2 To the extent that any Processing of Client Personal Data under this DPA involves an EU Restricted Transfer from Client to Nisos, the Parties shall comply with their respective obligations set out in the EU SCCs. The following Modules of the EU SCCs apply in the manner set out below:

(a) Module One of the EU SCCs applies to any EU Restricted Transfer involving Service Data; and/or

(b) Module Two of the EU SCCs applies to any EU Restricted Transfer involving Client Personal Data.

*UK Restricted Transfers*

6.3 To the extent that any Processing of Client Personal Data under this DPA involves a UK Restricted Transfer from Client to Nisos:

(a) the relevant EU SCCs entered into in accordance with Paragraph 6.2 of this Annex 1 (European Annex) shall apply to that UK Restricted Transfer as varied by the UK Addendum; and

(b) the Parties agree that the manner of the presentation of the information included in the UK Addendum shall not operate or be construed so as to reduce the Appropriate Safeguards (as defined in Section 3 of Part 2 of the UK Addendum).

*Adoption of new transfer mechanism*

6.4 Nisos may on notice vary this DPA and replace the relevant Data Transfer Mechanism(s) with:

(a) any new form, version, or module of the relevant Data Transfer Mechanism(s) or any replacement therefor prepared and populated accordingly; or

(b) another transfer mechanism, other than the current Data Transfer Mechanism(s), that enables the lawful transfer of Client Personal Data to Nisos under this DPA in compliance with Chapter V of the GDPR.

[REMAINDER OF PAGE INTENTIONALLY BLANK]

**Attachment 1 OF EUROPEAN ANNEX**

**DATA PROCESSING DETAILS**

**Note:**

This Attachment 1 of Annex 1 (European Annex) to the DPA includes certain details of the Processing of Personal Data as required:

- by Article 28(3) GDPR; and
- to populate the Appendices to the EU SCCs and UK Addendum.

## PART 1: DETAILS OF THE PARTIES

### NISOS / 'DATA IMPORTER' DETAILS

| | |
|---|---|
| **Name:** | Nisos (as set out in the pre-amble to the DPA) |
| **Address:** | As set out in the Order Form |
| **Contact Details for Data Protection:** | privacy@legal.com |
| **Nisos Activities:** | Nisos is a managed intelligence company that uses its proprietary technology and methodology to help clients proactively identify threats to their businesses. |
| **Role:** | *In respect of Client Personal Data:* Processor<br>*In respect of Service Data:* Controller |

### CLIENT / 'DATA EXPORTER' DETAILS

| | |
|---|---|
| **Name:** | Client (as set out in the pre-amble to the DPA) |
| **Address:** | As set out in the Order Form |
| **Contact Details for Data Protection:** | As set out in the Order Form |
| **Client Activities:** | Client's activities relevant to this DPA are the use and receipt of the Services under and in accordance with, and for the purposes |

| | |
|---|---|
| | anticipated and permitted in, the Order Form as part of its ongoing business operations. |
| **Role:** | Controller |

**PART 2: DETAILS OF NISOS' PROCESSING AS A PROCESSOR**

| | |
|---|---|
| **Categories of Data Subjects:** | Any individuals whose Personal Data is comprised within data submitted to the Services by or on behalf of Client under the Order Form, and/or obtained by Nisos in its performance of the Services – but may include:<br>● Client's and its affiliates' and target companies':<br>○ staff;<br>○ customers, clients, (sub-)licensees, users and end-users, website visitors and marketing prospects;<br>○ suppliers, service providers, consultants, advisers and other providers of goods or services;<br>○ distributors, resellers, sales agents, introducers, sales representatives, collaborators, joint-venturers and other commercial partners;<br>○ shareholders, partners, members and supporters; and<br>○ advisers, consultants and other professionals and experts.<br>● Data Subjects identified by Nisos as part of Nisos' threat detection.<br>Where any of the above is a business or organisation, it includes their staff.<br>Each category includes current, past and prospective Data Subjects. |
| **Categories of Personal Data:** | Any Personal Data comprised within data submitted to the Services by or on behalf of Client under the Order Form, and/or obtained by Nisos in its performance of the Services – but may include:<br>● Personal details, including any information that identifies the Data Subject and their personal characteristics, including: name, address, contact details (including email address, |

| | |
|---|---|
| | telephone details and other contact information), age, date of birth, sex, and physical description.<br>● User endpoint behaviour (including user account activity and metadata, applications executed on endpoints, and accessed URLs).<br>● Technological details, such as internet protocol (IP) addresses, unique identifiers and numbers (including unique identifier in tracking cookies or similar technology), pseudonymous identifiers, precise and imprecise location data, internet / application / program activity data, and device IDs and addresses.<br>● Any Personal Data relevant to a threat, both actual and suspected. |
| **Sensitive Categories of Data, and associated additional restrictions/safeguards:** | Categories of sensitive data:<br>As noted in Section 8.4 of the DPA, Client agrees that Restricted Data, which includes 'sensitive data' (as defined in Clause 8.7 of the EU SCCs), must not be submitted to the Services unless otherwise agreed in the Order Form. Where Client provides Restricted Data to Nisos, the details of such Restricted Data shall be included in the Order Form.<br>Additional safeguards for sensitive data:<br>N/A |
| **Frequency of transfer:** | Ongoing. |
| **Nature of the Processing:** | Processing operations required in order to provide the Services in accordance with the Order Form. |
| **Purpose of the Processing:** | Client Personal Data will be processed: (i) as necessary to provide the Services as initiated by Client in its use thereof, and (ii) to comply with any other reasonable instructions provided by Client in accordance with the terms of this DPA. |
| **Duration of Processing / Retention Period:** | For the period determined in accordance with the Order Form and DPA, including Paragraph 4 of Annex 1 (European Annex) to the DPA. |
| **Transfers to (sub-)processors:** | Transfers to Sub-Processors are as, and for the purposes, described from time to time in the Sub-Processor List (as may be updated from time to time in accordance with Paragraph 2 of Annex 1 (European Annex) to the DPA). |

## PART 3: DETAILS OF NISOS' PROCESSING AS A CONTROLLER

| | |
|---|---|
| **Categories of Data Subjects:** | Any individuals whose Personal Data is comprised within data submitted to the Services by or on behalf of Client under the Order Form, and/or obtained by Nisos in its performance of the Services – but may include Data Subjects identified by Nisos as part of Nisos' threat detection. |
| **Categories of Personal Data:** | Any Personal Data comprised within data submitted to the Services by or on behalf of Client under the Order Form, and/or obtained by Nisos in its performance of the Services – but may include:<br>● Personal details, including any information that identifies the Data Subject and their personal characteristics, including: name, address, contact details (including email address, telephone details and other contact information), age, date of birth, sex, and physical description.<br>● User endpoint behaviour (including user account activity and metadata, applications executed on endpoints, and accessed URLs).<br>● Technological details, such as internet protocol (IP) addresses, unique identifiers and numbers (including unique identifier in tracking cookies or similar technology), pseudonymous identifiers, precise and imprecise location data, internet / application / program activity data, and device IDs and addresses.<br>● Any Personal Data relevant to a threat, both actual and suspected. |
| **Sensitive Categories of Data, and associated additional restrictions/safeguards:** | Categories of sensitive data:<br>None – as noted in Section 8.4 of the DPA, Client agrees that Restricted Data, which includes 'sensitive data' (as defined in Clause 8.7 of the EU SCCs), must **not** be submitted to the Services.<br>Additional safeguards for sensitive data:<br>N/A |
| **Frequency of transfer:** | Ongoing. |
| **Nature of the Processing:** | Processing operations required in order to provide, improve, develop, optimise and maintain the Services. |

| | |
|---|---|
| **Purpose of the Processing:** | Service Data is Processed to provide, improve, develop, optimise and maintain the Services. |
| **Duration of Processing / Retention Period:** | For as long as necessary to achieve the purposes of the Processing. |
| **Transfers to (sub-)processors:** | Nisos shall comply with Applicable Data Protection Laws when appointing Processors to Process Service Data. |

## Attachment 2 OF EUROPEAN ANNEX

## EU SCCs

## <u>SECTION I</u>

### *Clause 1*

### ***Purpose and scope***

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

(b) The Parties:

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

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

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

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

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

### *Clause 2*

### ***Effect and invariability of the Clauses***

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

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

*Clause 3*

### ***Third-party beneficiaries***

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e);
(iv) Clause 12 - Module One: Clause 12(a) and (d); Module Two: 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 – Optional*

***Docking clause***

**[NOT USED]**

## SECTION II – OBLIGATIONS OF THE PARTIES

*Clause 8*

***Data protection safeguards***

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

**MODULE ONE: Transfer controller to controller**

### 8.1 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

### 8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer.

In the latter case, the data importer shall, to the extent possible, make the information publicly available.

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

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.3 Accuracy and data minimisation**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

**8.4 Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

**8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

### 8.6 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 or offences (hereinafter “sensitive data”), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

### 8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

### 8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

### 8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

## MODULE TWO: Transfer controller to processor

### 8.1 Instructions

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

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

### 8.2 Purpose limitation

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

### 8.3 Transparency

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

### 8.4 Accuracy

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

### 8.5 Duration of processing and erasure or return of data

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

### 8.6 Security of processing

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

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

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

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

### 8.7 Sensitive data

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

### 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the

European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

### 8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

## *Clause 9*

## ***Use of sub-processors***

**MODULE TWO: Transfer controller to processor**

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

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least for the time period set out at Section 2.3 of Annex 1 of the DPA in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

*Clause 10*

### ***Data subject rights***

**MODULE ONE: Transfer controller to controller**

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

**MODULE TWO: Transfer controller to processor**

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

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

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

*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***

**MODULE ONE: Transfer controller to controller**

(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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

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

**MODULE TWO: Transfer controller to processor**

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

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

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

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

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

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

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

*Clause 13*

***Supervision***

(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.

## <u>SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES</u>

*Clause 14*

***Local laws and practices affecting compliance with the Clauses***

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

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

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

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

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

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

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

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

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

*Clause 15*

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

**15.1 Notification**

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

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

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

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

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

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

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

**15.2 Review of legality and data minimisation**

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

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

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

## SECTION IV – FINAL PROVISIONS

*Clause 16*

### *Non-compliance with the Clauses and termination*

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

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

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

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
(ii) the data importer is in substantial or persistent breach of these Clauses; or
(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

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

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

*Clause 17*

### ***Governing law***

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

*Clause 18*

### ***Choice of forum and jurisdiction***

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

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

(g) 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.

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

## ANNEX I

### A. LIST OF PARTIES

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**DATA EXPORTER**:

**Name**: Client (as set out in Part 1 of Attachment 1 of Annex 1 (European Annex)).

**Address**: as set out in Part 1 of Attachment 1 of Annex 1 (European Annex)**.**

**Contact person's name, position and contact details**: as set out in Part 1 of Attachment 1 of Annex 1 (European Annex).

**Activities relevant to the data transferred under these Clauses**: as set out in Part 1 of Attachment 1 of Annex 1 (European Annex).

**Signature and date**: these Clauses are hereby deemed to be entered into by Client under and in accordance with Paragraph 6.2 of Annex 1 (European Annex) with effect from the Addendum Effective Date.

**Role (controller/processor)**: as set out in Part 1 of Attachment 1 of Annex 1 (European Annex).

**DATA IMPORTER**:

**Name**: Nisos (as set out in Part 1 of Attachment 1 of Annex 1 (European Annex)).

**Address**: as set out in Part 1 of Attachment 1 of Annex 1 (European Annex).

**Contact person's name, position and contact details**: as set out in Part 1 of Attachment 1 of Annex 1 (European Annex).

**Activities relevant to the data transferred under these Clauses**: as set out in Part 1 of Attachment 1 of Annex 1 (European Annex).

**Signature and date**: these Clauses are hereby deemed to be entered into by Nisos under and in accordance with Paragraph 6.2 of Annex 1 (European Annex) with effect from the Addendum Effective Date.

**Role (controller/processor)**: as set out in Part 1 of Attachment 1 of Annex 1 (European Annex).

## B. DESCRIPTION OF TRANSFER

### MODULE ONE: Transfer controller to controller

**Categories of data subjects whose personal data is transferred:** as set out in Part 3 of Attachment 1 of Annex 1 (European Annex).

**Categories of personal data transferred**: as set out in Part 3 of Attachment 1 of Annex 1 (European Annex).

**Sensitive data transferred (if applicable) and applied restrictions or safeguards**: as set out in Part 3 of Attachment 1 of Annex 1 (European Annex).

**The frequency of the transfer**: as set out in Part 3 of Attachment 1 of Annex 1 (European Annex).

**Nature of the processing**: as set out in Part 3 of Attachment 1 of Annex 1 (European Annex).

**Purpose(s) of the data transfer and further processing**: as set out in Part 3 of Attachment 1 of Annex 1 (European Annex).

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**: as set out in Part 3 of Attachment 1 of Annex 1 (European Annex).

**For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing**: as set out in Part 3 of Attachment 1 of Annex 1 (European Annex).

### MODULE TWO: Transfer controller to processor

**Categories of data subjects whose personal data is transferred:** as set out in Part 2 of Attachment 1 of Annex 1 (European Annex).

**Categories of personal data transferred**: as set out in Part 2 of Attachment 1 of Annex 1 (European Annex).

**Sensitive data transferred (if applicable) and applied restrictions or safeguards**: as set out in Part 2 of Attachment 1 of Annex 1 (European Annex).

**The frequency of the transfer**: as set out in Part 2 of Attachment 1 of Annex 1 (European Annex).

**Nature of the processing**: as set out in Part 2 of Attachment 1 of Annex 1 (European Annex).

**Purpose(s) of the data transfer and further processing**: as set out in Part 2 of Attachment 1 of Annex 1 (European Annex).

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**: as set out in Part 2 of Attachment 1 of Annex 1 (European Annex).

**For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing**: as set out in Part 2 of Attachment 1 of Annex 1 (European Annex).

## C. COMPETENT SUPERVISORY AUTHORITY

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

The Data Protection Commissioner of Ireland.

## ANNEX II

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

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

As set out in Annex 2 (Security Measures) of the DPA.

NISOS

## Attachment 3 OF EUROPEAN ANNEX

## UK ADDENDUM

## International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

## VERSION B1.0, in force 21 March 2022

This UK 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*

All relevant information and details are as set out in Part 1 of Attachment 1 of Annex 1 (European Annex) to the DPA and it is noted that the UK Addendum is deemed to have been signed by the Parties pursuant to and in accordance with Paragraph 6.3 of Annex 1 (European Annex) with effect from the Addendum Effective Date.

### *Table 2: Selected SCCs, Modules and Selected Clauses*

The version of the Approved EU SCCs which this UK Addendum is appended to, detailed below, including the Appendix Information:

| |
|---|
| **Date:** Addendum Effective Date |
| **Reference (if any):** the EU SCCs |
| **Other identifier (if any):** n/a |

### *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 UK Addendum is set out in:

| |
|---|
| **Annex 1A: List of Parties:** Part 1 of Attachment 1 of Annex 1 (European Annex) |
| **Annex 1B: Description of Transfer:** Part 2 and Part 3 of Attachment 1 of Annex 1 (European Annex) |

| |
|---|
| **Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:** Annex 2 |
| **Annex III: List of Sub processors (Modules 2 and 3 only):** n/a |

*Table 4: Ending this UK Addendum when the Approved Addendum Changes*

| |
|---|
| **Which Parties may end this UK Addendum as set out in Section 19:** Importer |

**Part 2: Mandatory Clauses**

The Mandatory Clauses are incorporated by reference and form a binding and effective part of this UK Addendum.

## Annex 2

## Security Measures

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

1. Organisational management and dedicated staff responsible for the development, implementation and maintenance of Nisos' information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Nisos' organisation, monitoring and maintaining compliance with Nisos' policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include at a minimum logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for Client Personal Data.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.

5. Password controls designed to manage and control password strength, expiration and usage.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Nisos' possession.

8. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to Nisos' technology and information assets.

9. Incident management procedures designed to allow Nisos to investigate, respond to, mitigate and notify of events related to Nisos' technology and information assets.

10. Network security controls that provide for the use of enterprise firewalls and intrusion detection systems designed to protect systems from intrusion and limit the scope of any successful attack.

11. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

12. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

## Annex 3

## Authorised Sub-Processors

| Sub-Processor | Function | Location |
|---|---|---|
| Auth0 | Identity and access management | 10800 NE 8th Street Suite 700 Bellevue, WA 9800, USA |
| Amazon Web Services | Storage and processing | 410 Terry Avenue North, Seattle, WA, USA |
| Gong | Recording sales calls | 265 Cambridge Ave, Suite 60717 Palo Alto, CA 94306, USA |
| Google Cloud Platform | Storage and APIs | 1600 Amphitheatre Pkwy, Mountain View, CA, USA |
| Google Workplace | Google services | 1600 Amphitheatre Pkwy, Mountain View, CA, USA |
| Hubspot | Marketing | HubSpot Inc. 25 First Street, Cambridge, MA 02141 USA |
| Kahootz | Client portal software-as-a-service provider | Weston Farm Barn, Newbury Road, Weston, Newbury, Berkshire, RG20 8JA, UK |
| Microsoft | Office365 | Microsoft Headquarters, One Microsoft Way Redmond, WA 98052, USA |
| Salesforce | Sales and marketing | 1442 Second St, Santa Monica, CA 90401, USA |
| Slack | Internal messaging | 500 Howard St, San Francisco, CA 94105, USA |
| Symphonic Source | Marketing data cleansing | 4004 Belt Line Road, Suite 120<br>Dallas, TX 75001 |
| Sumo Logic | System and audit log storage and analysis | 305 Main Street, Redwood City, CA 94063, USA |

**If you would like more information about additional Sub-Processors who Process Client Personal Data with respect to the specific Services that you use, please reach out to your designated Customer Success Director or email privacy@nisos.com.*