TOKENEX, INC.
DATA PROCESSING ADDENDUM

This **Data Processing Addendum** ("Addendum") is an amendment to the contract (collectively, the "Agreement") entered into between TokenEx Inc. ("TokenEx") and the Customer that is a party to this Addendum and is effective as of the date of last signature to this Addendum ("Effective Date").

In consideration of the mutual obligations in this Data Processing Addendum, the parties agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1. All terms defined in the Agreement shall be deemed to have the same meaning in this Addendum, other than any specifically defined in or amended by this Addendum. Any term that is defined in Data Protection Legislation but not defined in this Addendum shall have the meaning set forth in the applicable Data Protection Legislation. This Addendum supersedes any prior addendum entered into between the parties, with respect to the subject matter hereof.

1.2. For purposes of this Addendum:

(a) **"ANPD"** means the National Data Protection Authority created by the LGPD.

(b) **"Data Controller"** shall mean the natural or legal person which alone or jointly with others determines the purposes and means of the Processing for the purposes of this Addendum.

(c) **"Data Processor"** shall mean any natural or legal person which processes Personal Data on behalf of and under the strict instructions of the Data Controller for the purposes of this Addendum.

(d) **"Data Protection Legislation"** means (i) Brazilian Data Protection Law (the "LGPD"); (ii) Regulation (EU) 2016/679 (the "GDPR"); (iii) the UK Data Protection Laws as defined in Attachment B to this Addendum (the "UK GDPR") and (iv) any other data protection or data privacy law and regulation that is applicable to Services, in each case along with any applicable secondary or supplementary legislation, as amended or updated from time to time, and any successor legislation, and amendments and re-enactments of the same, including where applicable the guidance, standards, rules and codes of practice issued by applicable regulatory authorities.

(e) **"Personal Data"** shall mean all information relating to an identified or identifiable natural person ("**Data Subject**" or **"Holder"**) that is Processed by the TokenEx as a Data Processor for Customer under this Addendum.

(f) **"Process," "Processed," or "Processing"** means any operation performed with personal data, such as those regarding the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation or control of information, modification, communication, transfer, diffusion or extraction.

(g) **"Third Party"** means any company, other than a TokenEx affiliate, which is engaged by TokenEx for the provision of the Services.

2. PROVISIONS RELATING TO PERSONAL DATA

2.1. The parties expressly agree that Customer is the Data Controller for the Personal Data Processed for the purpose of the provision of the Services under this Addendum. Customer, as Data Controller, shall ensure that any Personal Data Processed by TokenEx on Customer's behalf for the purposes of this Addendum is Processed in accordance with the Data Protection Legislation. Accordingly, Customer expressly guarantees:

(a) any Personal Data is Processed on the basis of an adequate legal ground as permitted under the Data Protection Legislation.

(b) any Personal Data is Processed for a defined, explicit and legitimate purpose.

(c) any Personal Data Processed is relevant and non-excessive in consideration of the purpose of the Processing.

(d) any Personal Data is and will be maintained accurate and up to date for the entire term of the provision of the Services under the Agreement.

(e) a term of retention has been defined for Personal Data, which is legitimate in consideration of the purpose of the Processing and the nature of Personal Data Processed.

(f) complete, clear and accurate information is provided to Data Subjects whose Personal Data is Processed under this Addendum, including, if relevant, information concerning the fact that Personal Data may be transferred outside the European Economic Area or other geographic area in which the Personal Data is collected.

(g) Data Subjects whose Personal Data is Processed under this Addendum are granted adequate and effective means to exercise their rights with regard to

Processing of their Personal Data in accordance with Data Protection Legislation (access, rectification, update, erasure, etc. as applicable). TokenEx shall not be liable in cases where Customer fails to respond to the Data Subject's request in total, correctly or in a timely manner.

(h) all adequate and necessary formalities, if any, or internal documentation, required by Data Protection Legislation, have been completed with all competent authorities, completed or otherwise retained internally by Customer.

(i) Customer has conducted all relevant verifications and obtained all relevant information which it deems necessary regarding TokenEx and is satisfied that TokenEx provides sufficient guarantees to Process Personal Data in accordance with the requirements of Data Protection Legislation.

(j) Customer shall maintain a current and up to date a register of data Processing activity and shall provide that register to TokenEx at least annually during the term of this Agreement.

2.2. Nothing in this Addendum or the Agreement shall relieve TokenEx of its own direct responsibilities and liabilities under the Data Protection Legislation.

2.3. **Customer Processing Instructions**.

2.3.1 As applicable, Attachments A, B and C of this Addendum, attached hereto and incorporated herein (the "**SCC Attachments**"), set forth contractual clauses required for compliance with GDPR and UK GDPR. If the GDPR Standard Contractual Clauses and the UK International Data Transfer Addendum (**"UK Addendum"**) are applicable to Services and the contract language contained in either are revised, amended or replaced by the relevant data protection authorities, the parties agree that the revised, amended or replacement language is added to or substituted in the place of the GDPR Standard Contractual Clauses or UK Addendum, as applicable, effective as of the date of adoption by such authorities and without further action on the part of either party.

2.3.2 Customer's documented instructions related to the Processing of Personal Data by TokenEx is set forth in the SCC Attachments, Appendix Annex I. TokenEx shall not Process Personal Data other than on Customer's documented instructions (including the Agreement) unless Processing is required by applicable law to which TokenEx is subject, in which case TokenEx shall, unless prohibited by applicable law, inform Customer of that legal requirement before the relevant Processing of that Personal Data. Should Customer wish to implement modifications to its instructions, Customer shall notify TokenEx in writing at least thirty (30) days in advance in order for both parties to evaluate Customer's proposed modification. Customer agrees that Personal Data may be used on an aggregated and anonymized basis to support and enhance security and

fraud prevention aspects of Services. For clarity, the instructions set forth in the SCC Attachments apply to Processing by TokenEx regardless of whether the GDPR or UK GDPR is applicable to Processing.

2.3.3 Customer hereby expressly acknowledges and accepts that TokenEx shall not be bound by any Customer instructions breaching applicable law (including Data Protection Legislation). As such, TokenEx shall be entitled to suspend performance on such instructions until Customer conforms or modifies such instructions. In such cases, TokenEx shall provide prior notice to the Customer of such intended suspension.

2.4. **TokenEx's roles and obligation.** The parties expressly agree that Customer is the Data Controller and TokenEx is the Data Processor in the event TokenEx collects or otherwise Processes (including to store) Personal Data on behalf of Customer when performing the Services. Accordingly, TokenEx will:

(a) ensure that all persons authorised by TokenEx to Process the Personal Data are under an enforceable obligation to keep Personal Data strictly confidential.

(b) adopt and maintain appropriate technical and organisational measures specified in the SCC Attachments, Appendix Annex II designed to ensure the Personal Data is kept secure, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, including but not limited to any specific measures agreed between Customer and TokenEx elsewhere in the Agreement.

(c) subject to Section 2.3 (Customer Processing Instructions), only transfer the Personal Data in accordance with any reasonable written instructions from Customer set forth in the SCC Attachments and take all further steps necessary to ensure that any data transfer is and remains in accordance with the Data Protection Legislation.

(d) without limitation and notwithstanding any other obligation under this Addendum, TokenEx shall, (and shall ensure that any sub-processor shall), on request, provide all information and assistance reasonably required by Customer to enable Customer to comply with the Data Protection Legislation in relation to Personal Data, to the extent TokenEx can reasonably have access to Personal Data with regard to the Processing by TokenEx. Notwithstanding the foregoing, TokenEx shall not respond to any Data Subject request, inquiry, complaint, or claim relating to Processing of Personal Data without Customer's prior written consent except to the extent required by the Data Protection Legislation or reasonably necessary to confirm that the request relates to Customer. TokenEx shall not be liable in cases where Customer fails to respond to the Data Subject's request in total, correctly or in a timely manner.

(e) ensure that TokenEx has adequate processes and systems in place to comply with its obligations under Section 2.4(d) above.

(f) (i) in sub-processor contracts, impose the same or substantially equivalent data protection obligations as stipulated in this Addendum and engage sub-processors who provide sufficient guarantees to implement appropriate technical and organisational measures designed to ensure Processing will meet the requirements of the Data Protection Legislation. TokenEx remains liable to the Customer for the data protection obligations of any sub-processor it engages, subject to the liability provisions of the Agreement.

(ii) Customer hereby grants specific authorization for TokenEx to engage sub-processors listed in the SCC Attachments, Appendix Annex III. TokenEx is generally authorized to engage additional sub-processors as necessary to perform the Processing, however TokenEx shall notify Customer prior to engaging any such sub-processor. Where Customer objects to TokenEx's use of such a sub-processor, Customer shall notify TokenEx in writing within five (5) business days after receipt of TokenEx's notification of its intent to engage the sub-processor. In the event Customer objects to a sub-processor, Customer may terminate this Addendum with thirty (30) days' notice, without penalty. If Customer terminates this Addendum as a result of such appointment or replacement of a sub-processor, any transition assistance services will be provided in accordance with the Agreement.

(g) except to the extent necessary to provide Services, not modify, amend or alter the contents of the Personal Data or disclose or permit the disclosure of any of the Personal Data to any third party unless specifically approved in advance in writing by Customer. Notwithstanding the foregoing sentence, Personal Data may be used on an aggregated and anonymized basis to support and enhance security and fraud prevention aspects of Services.

(h) immediately notify Customer with full details if TokenEx:

(i) becomes aware of any breach of the Data Protection Legislation in relation to the Agreement; or

(ii) subject to Section 2.4(d), receives any request (including from a Data Subject or the data protection regulator) to disclose any Personal Data; provided TokenEx shall not directly respond to such requests except as duly and expressly agreed between the parties as part of the Services under the Agreement.

(i) upon no less than sixty (60) days' written notice by Customer:

(i) make available to Customer all such information as is reasonably necessary to demonstrate TokenEx's compliance with Data Protection Legislation;

(ii) allow Customer to carry out or have an independent duly appointed third party for its auditing functions, any of whom shall be bound by a strict obligation of confidentiality, to perform an audit of TokenEx's Processing facilities in order to ensure compliance with obligations set forth in this Addendum. TokenEx shall be entitled to reject third party auditors which are competitors of TokenEx. Such audit operations shall not exceed a period of twelve (12) hours per year, shall occur not more than once per year, shall not hinder or otherwise disrupt in any way TokenEx's operations or business activities and shall only relate to that part of the relevant infrastructure which Processes Customer's Personal Data. TokenEx's assistance in relation to such activity shall be invoiced at TokenEx's then applicable rates; and

(iii) provide, at Customer's cost and during normal business hours, all reasonable cooperation, access and assistance in the carrying out any required audit and allow Customer the right to take copies of the records or any information relevant to its audit.

(j) notwithstanding any agreed retention periods applicable to Personal Data in this Addendum, on termination of the Agreement, at Customer's sole election, TokenEx will provide all Personal Data to Customer and/or permanently delete such Personal Data, save where applicable law allows or requires TokenEx to retain Personal Data, in which case TokenEx shall provide Customer with written particulars of any Personal Data so retained. This sub-clause 3.4(j) will survive termination of the Agreement.

2.5. **Transfers of Customer Personal Data to Third Party Countries.** Customer expressly acknowledges and accepts that Personal Data may be transferred and/or Processed outside the European Economic Area or other geographic area in which Personal Data is collected. TokenEx agrees to comply with the required contractual clauses set forth in the SCC Attachments. Accordingly, Customer hereby expressly consents that Personal Data may be transferred to TokenEx.

2.6. **Compliance with Data Protection Legislation.** TokenEx warrants to Customer and Customer warrants to TokenEx that each will fully comply with the provisions of the Data Protection Legislation in carrying out its obligations under this Addendum.

IN WITNESS WHEREOF, Customer and TokenEx, each through its duly authorized representative, hereby agree to the provisions of this Data Processing Addendum.

CUSTOMER	**TOKENEX, INC.**
[insert name]	
_____	_____
[insert signatory name/title]	Jeffrey Rudd, Chief Financial Officer
_____	_____
Date	Date

ATTACHMENT A TO

TOKENEX, INC. DATA PROCESSING ADDENDUM

GDPR STANDARD CONTRACTUAL CLAUSES

Data Controller to Data Processor – Processing in EU

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

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

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

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

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

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

Clause 2

Invariability of the Clauses

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

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

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

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

Clause 4

Hierarchy

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

Clause 5

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a Data Controller or a Data Processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a Data Controller or a Data Processor, in accordance with its designation in Annex I.

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

[Remainder of Page Intentionally Left Blank]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

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

Clause7

Obligations of the Parties

7.1. Instructions

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

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

7.2. Purpose limitation

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

7.3. Duration of the processing of personal data

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

7.4. Security of processing

(a) The Data Processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

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

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the Data Processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

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

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

(c) The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the Data Controller's request, the Data Processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Data Controller may take into account relevant certifications held by the Data Processor.

(d) The Data Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Data Processor and shall, where appropriate, be carried

out with reasonable notice.

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

7.7. Use of sub-processors

(a) The Data Processor has the Data Controller's general authorisation for the engagement of sub-processors from an agreed list. The Data Processor shall specifically inform in writing the Data Controller of any intended changes of that list through the addition or replacement of sub-processors at least thirty (30) calendar days in advance, thereby giving the Data Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The Data Processor shall provide the Data Controller with the information necessary to enable the Data Controller to exercise the right to object.

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

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

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

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

7.8. International transfers

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

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

Clause 8

Assistance to the Data Controller

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

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

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

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

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

(3) the obligation to ensure that personal data is accurate and up to date, by informing the Data Controller without delay if the Data Processor becomes aware that the

personal data it is processing is inaccurate or has become outdated;

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

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

Clause 9

Notification of personal data breach

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

9.1 Data breach concerning data processed by the Data Controller

In the event of a personal data breach concerning data processed by the Data Controller, the Data Processor shall assist the Data Controller:

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

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

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

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

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

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

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

9.2 Data breach concerning data processed by the Data Processor

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

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

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

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

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

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

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

.

ATTACHMENT B TO
TOKENEX, INC. DATA PROCESSING ADDENDUM

UK GDPR INTERNATIONAL DATA TRANSFER ADDENDUM
TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

Table 1: Parties

Start date	the Order effective date	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: TokenEx, Inc. Trading name (if different): NA Main address (if a company registered address): 3825 Northwest 166 Street, Suite C1, Edmond, OK 73012 Official registration number (if any) (company number or similar identifier): NA
Key Contact	Full Name (optional): see Appendix Annex I to SCC Attachments Job Title: see Appendix Annex I to SCC Attachments	Full Name (optional): See Appendix Annex I to SCC Attachments Job Title: See Appendix Annex I to SCC Attachments

	Contact details including email: see Appendix Annex I to SCC Attachments	Contact details including email: See Appendix Annex I to SCC Attachments
Signature (if required for the purposes of Section 2)	NA	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: effective date of the Order Reference (if any): Module 2 Other identifier (if any): NA

Table 3: Appendix Information

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

Annex 1A: List of Parties: see Appendix Annex I to SCC Attachments
Annex 1B: Description of Transfer: see Appendix Annex I to SCC Attachments
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: see Appendix Annex II to SCC Attachments
Annex III: List of Sub Data Processors (Modules 2 and 3 only): see Appendix Annex III to SCC Attachments

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

Entering into this Addendum

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

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.

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

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

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

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

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

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

Hierarchy

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

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

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

Incorporation of and changes to the EU SCCs

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

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

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

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

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

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

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

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

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from Data Controllers to Data Processors and/or Data Processors to Data Processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

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

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

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

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

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

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

    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

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

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

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

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

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

m. Clause 17 is replaced with:

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

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

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

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

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

    b its risk under the Addendum,

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

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

ATTACHMENT C TO

TOKENEX, INC. DATA PROCESSING ADDENDUM

GDPR STANDARD CONTRACTUAL CLAUSES

Data Controller to Data Processor – **Transfer of Data to Third Country**

SECTION I

Clause 1

Purpose and scope

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

(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 Data Controllers to Data Processors and/or Data Processors to Data 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 – Clause 8.1(b), 8.9(a), (c), (d) and (e);
- (iii) Clause 9 – Clause 9(a), (c), (d) and (e);
- (iv) Clause 12 – Clause 12(a), (d) and (f);
- (v) Clause 13;
- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e);
- (viii) Clause 18 – 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 Appendix Annex I.

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Appendix Annex I, 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 Appendix 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 Appendix Annex I. 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 Appendix 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 Appendix Annex I and/or Annex II.

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

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered

by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) calendar days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

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

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

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a Data Processor acting on behalf of a Data Controller, to the liability of the Data 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 Appendix Annex I, 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 Appendix Annex I, 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 Appendix Annex I, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the

essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

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

(ii) 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.

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

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

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

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

APPENDIX TO
SCC ATTACHMENTS TO
TOKENEX, INC. DATA PROCESSING ADDENDUM

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

APPENDIX ANNEX I TO
SCC ATTACHMENTS TO
TOKENEX, INC. DATA PROCESSING ADDENDUM

PERSONAL DATA PROCESSING

This Annex forms part of the Data Processing Addendum and is effective as of the Data Processing Addendum Effective Date.

A. LIST OF PARTIES

Data exporter(s):

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

☒ Data tokenization and detokenization services

☐ Account updates to credit card information

☐ Network tokenization services regarding account updates to credit card information

☐ Secure hosting of tokenized personal data

☐ 3D Secure fraud detection services

Data Exporter Signature:

_____

Name and Title:

Role (Data Controller/Data Processor): Data Controller

Data importer(s):
Name: TokenEx, Inc., a U.S.-based supplier of data tokenization services

Address: 3825 Northwest 166 Street, Suite c1, Edmond, Oklahoma 73012

Contact person's name, position and contact details:

Data Protection Officer, at legal@tokenex.com

Activities relevant to the data transferred under these Clauses:

☒ Data tokenization and detokenization services

☐ Account updates to credit card information

☐ Network tokenization services regarding account updates to credit card information

☐ Secure hosting of tokenized personal data

☐ 3D Secure fraud detection services

Data Importer Signature:

_____

Name and Title: Jeffrey Rudd, Chief Financial Officer

Role (Data Controller/Data Processor): Data Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of personal data transferred

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

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

Continuous basis

Nature of the processing

Processing of personal data may include receiving data including collection, accessing, retrieval, recording and data entry; holding data including storage, organization and structuring; using data including analysing, consultation, testing, automated decision-making and profiling; updating data including correcting, adaptation, alteration, alignment and combination; protecting data including restricting, encrypting and tokenizing; sharing data including disclosure,

dissemination, allowing access or otherwise making available; returning data; erasing data or other processing as instructed by Customer.

Purpose(s) of the data transfer and further processing

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

As applicable, until the later of the duration necessary for data exporter to provide business services to its customers; Agreement expiration; all Services provided under the Agreement are terminated, including the period allowed after Agreement expiration or termination for return of personal data; or for the establishment, exercise or defence of legal claims.

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

Microsoft is a sub-processor used for secure hosting services via Microsoft Azure data centers until the later of Agreement expiration or all services provided under the Agreement are terminated.

TSYS is a sub-processor used for the service to update credit card information if the data exporter subscribes to the Account Updater Service, until the later of Agreement expiration or all Account Updater services provided under the Agreement are terminated.

Bell Identification B. V. is a sub-processor used to provide network tokenization services to update changes to credit card information automatically if the data exporter subscribes to the Network Tokenization Service, until the later of Agreement expiration or all network tokenization services provided under the Agreement are terminated.

Mastercard Europe SA is a sub-processor used to provide 3D Secure fraud detection services if the data exporter subscribes to the 3D Secure Service, until the later of Agreement expiration or all 3D Secure services provided under the Agreement are terminated.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of the GDPR Standard Contractual Clauses.

APPENDIX ANNEX II TO
SCC ATTACHMENTS TO
TOKENEX, INC. DATA PROCESSING ADDENDUM

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

This Annex forms part of the Data Processing Addendum and is effective as of the Data Processing Addendum Effective Date.

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

Technical measures include but are not limited to:

The data importer's data protection platform is architected for high availability at each layer of the technology stack and prioritizes at the highest level a short recovery time objective and recovery point objective if an incident involves restoring availability. To address the need for availability and access to personal data in event of a physical or technical incident, a Microsoft Azure data center is used for secure off-site hosting, with failover to a secondary data center. The data importer also logs all events for platform performance, availability, security and uptime using an immutable logging platform for aggregation and alerting.

Personal data is encrypted at rest and in transit using industry standard encryption methods and processing by the data importer utilizes a format preserving encryption to tokenize (or detokenize) the personal data, at the instruction of the data exporter.

The data importer has ISO 27001, PCI-DSS and SSAE 18 SOC 2 Type II certifications and regular third-party audits associated with the certifications. The data importer adheres to the GDPR Code of Conduct and, although the Privacy Shield (EU-US and Swiss-US) was invalidated as the sole source of adequacy for cross border data transfers with the European Union, the data importer continues to maintain the level of commitment to data protection safeguards for which the Privacy Shield was created.

Regarding user identification and authentication, the data importer uses a combination of unique ID and API key for authorization and multi-factor authentication for user identification.

The data importer has disaster recovery and business continuity plans which include incident response and are tested at least annually. The data importer also maintains internal processes for regular testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure security of the processing.

Additional technical measures are: use of CIS secure baseline configurations, applied with group policy to ensure configurations consistently adhere to CIS standards; quarterly external and internal vulnerability scanning; annual external and internal application pen testing; internal audits related to ISO 27001 audit; and quarterly access, configuration and firewall reviews; automated alerting for traffic to and from the platform to identify potentially malicious anomalies; external threat intelligence sources; and 24/7 endpoint detection and response monitoring.

The Service Level Agreement of the data importer is located online at Legal | TokenEx | Cloud Tokenization & Data Vault Services.

Organisational measures include but are not limited to:

Personal data subject to processing by TokenEx is provided by or on behalf of the data exporter and all manner of processing personal data and compliance with legal obligations to data subjects is performed pursuant to and limited by data exporter instructions. The data exporter determines the data collected, stored and retention period and controls data portability and erasure processing.

The data importer adheres to the GDPR Code of Conduct and, although the Privacy Shield (EU-US and Swiss-US) was invalidated in 2020 as the sole source of adequacy for cross border data transfers with the European Union, the data importer continues to maintain the level of commitment to data protection safeguards for which the Privacy Shield was created.

In addition to third-party audits described above, the data importer performs internal GRC assessments and maintains an active Governance, Risk and Compliance program. The GRC program includes cross-department involvement

and is comprised of committees that perform quarterly reviews in the areas of Privacy; Vendor Management; Security and Compliance.

The data importer has disaster recovery and business continuity plans which include incident response and are tested at least annually. The data importer also maintains internal processes for regular testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure security of the processing.

Sub-Data Processors are required to have sufficient technical and organisational security safeguards designed to ensure the confidentiality, integrity and availability of personal data and the same level of protection as provided by the data importer to the data exporter.

APPENDIX ANNEX III TO
SCC ATTACHMENTS TO
TOKENEX, INC. DATA PROCESSING ADDENDUM

AGREED LIST OF SUB-DATA PROCESSORS

This Annex forms part of the Data Processing Addendum and is effective as of the Data Processing Addendum Effective Date.

Data Controller provides general authorisation for the engagement of sub-processors and specific authorisation of sub-processors is not required but pursuant to the agreed list referenced in Clause 9(a), the Data Controller and Data Processor agree to the following list:

1. Microsoft Azure data centers for secure hosting services.
2. TSYS, if the Account Updater service for updating credit card information is included in Services.
3. Bell Identification B. V., if the Network Tokenization service for account changes to credit card information is included in Services.
4. Mastercard Europe SA, if the 3D Secure service for fraud detection is included in Services.

---

[i] Where the data exporter is a Data Processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as Data Controller, reliance on these Clauses when engaging another Data Processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the Data Controller and the Data Processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the Data Controller and Data Processor rely on the standard contractual clauses included in Decision 2021/915.

[ii] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway.

The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[iii] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[iv] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.