DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**Addendum**") forms an integral part of the Master Service Agreement (the "**Agreement**") or any other agreement(s), order(s), statement(s) of work, or other legally binding instrument(s) in connection with the provision of Services by and between AU10TIX Ltd. ("**Au10tix**") the provider of Services under the Agreement, and the recipient of the Services under the Agreement ("**Customer**"). Each of Au10tix and Customer a "**Party**" and collectively the "**Parties**".

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect. The exhibits, annexes, appendices, and schedules attached to this Addendum (each an "**Annex**") form an integral part hereof and are expressly incorporated herein by this reference.

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

1. Definitions and Interpretation

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

1.1.1 "**BIPA**" means the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq.;

1.1.2 "**CPRA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (CCPA), as amended by the California Privacy Rights Act of 2020, and its implementing regulation;

1.1.3 "**Customer Personal Data**" means any Personal Data or Personal Information Processed by Au10tix on behalf of Customer pursuant to or in connection with the Agreement;

1.1.4 "**Data Protection Laws**" means applicable laws, regulations and regulatory guidance containing rules for the protection of individuals with regard to the Processing of Personal Data, including (to the extent applicable to the relevant Party) the GDPR, the UK GDPR and the CPRA;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.7 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Au10tix for Customer pursuant to the Agreement, including as described in **Annex I**;

1.1.8 "**Standard Contractual Clauses**" means the Standard Contractual Clauses attached as **Schedule 3**. Should any subsequent version thereof be released by the European Commission, **Schedule 3** shall be amended accordingly;

1.1.9 "**Sub-processors**" means any person (including any third party, but excluding an employee of Au10tix or any of its affiliates) appointed by or on behalf of Au10tix to Process Personal Data in connection with the Agreement.

1.2 The terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Process**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly. The term "**Personal Information**" shall have the same meaning as in the CPRA.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. **Processing of Customer Personal Data**

2.1 Au10tix will Process Customer Personal Data as a Processor, in accordance with Customer's documented instructions, unless Processing is required by applicable laws to which Au10tix is subject, in which case Au10tix will, to the extent permitted by applicable laws, inform the Customer of that legal requirement before the relevant Processing of that Personal Data.

2.2 Customer hereby:

2.2.1 instructs Au10tix (and authorizes Au10tix to instruct each Sub-processors) to Process Customer Personal Data (including, by transferring Customer Personal Data to any country or territory) as reasonably necessary for the provision of the Services or as otherwise instructed by the Customer as part of the Services, and in accordance with this Addendum; and

2.2.2 warrants and represents that it is and will at all relevant times remain (a) duly and effectively authorized to give the instruction set out in section 2.2.1; (b) the Controller of the Customer Personal Data Processed by Au10tix; (c) responsible for and in compliance with its obligations as a Controller of Customer Personal Data under applicable law (including the Data Protection Laws), in particular with respect to the justification of any Processing of Customer Personal Data by Au10tix and/or any Sub-processors; and (d) entitled to provide Customer Personal Data to Au10tix.

2.3 **CPRA Specific Provisions**. To the extent that the CPRA applies to the Processing of Customer Personal Data by Au10tix, the following provisions apply to such processing:

2.3.1 Customer and Au10tix acknowledge that: **(A)** Customer Personal Data is disclosed to Au10tix only for the following the limited Business Purpose of providing Customer with the Services (the "**Purpose**"); and, **(B)** Customer is not Selling Customer Personal Data to Au10tix.

2.3.2 Au10tix will notify Customer of any valid request received from an Individual pursuant to CPRA that Customer must comply with, and will provide all information necessary for Customer to comply with such request.

2.3.3 Au10tix will: **(A)** comply with all provisions under CPRA applicable to Au10tix, including with respect to providing the same level of protection to privacy as required under CPRA; and, **(B)** notify Customer no later than within five (5) business days after determining that Au10tix can no longer meet its obligations under CPRA, to the extent that the CPRA applies to the Processing of Customer Personal Data by Au10tix.

2.3.4 Au10tix will not: **(A)** Sell Customer Personal Data or Share (within the meaning thereof under the CPRA) Customer Personal Data or retain Customer Personal Data for any purpose other than for the Purpose or outside of the direct business relationship between Customer and Au10tix as detailed under this Addendum and the Agreement, except as permitted under CPRA; and, **(B)** unless otherwise permitted under CPRA, retain, use, or disclose Customer Personal Data: **(i)** for any purposes other than those specified under this Addendum; **(ii)** for any commercial purpose other than the Purpose, including in providing services to other customers of Au10tix; or, **(iii)** outside the direct business relationship between Customer and Au10tix.

2.3.5 Customer may: **(A)** take reasonable and appropriate steps to ensure that Au10tix uses Customer Personal Data in a manner consistent with Customer's obligations under CPRA; **(B)** upon notice, take reasonable and appropriate steps to stop and remediate Au10tix's unauthorized use of Customer Personal Data.

2.4 Notwithstanding the above, Customer will be solely responsible for: **(a)** providing any required notices, obtaining and documenting any required consents and/or authorizations to/from Data Subjects and/or other third parties, including obtaining explicit consent to the processing of special categories of data, all in accordance with Articles 7-9 and 12-14 of the GDPR, and obtaining and documenting the explicit consent, or written release of the individuals who are the subject of the biometric data used by Au10tix as part of its Services to the Customer, for their use of their biometric data, in accordance provisions under applicable laws related to biometric data, including without limitation section 15(b) of the BIPA, and further refer such individuals to the Au10tix's Biometric Data Policy, which is available at: https://www.au10tix.com/biometric-data-policy/ ; **(b)** securing an appropriate legal basis under

applicable law (including the Data Protection Laws), as necessary for Au10tix to Process Customer Personal Data as a Processor on Customer's behalf (including Processing under **Schedule 3** where applicable); **(c)** ensuring that Company Personal Data is accurate and up to date; and **(d)** Customer's decisions and actions concerning the Processing of such Customer Personal Data. Au10tix will inform Customer, if in its opinion any Customer's instruction violates any provision under Data Protection Laws, and will be under no obligation to follow such instruction, until the matter is resolved following a good-faith discussion between the Parties

3. **Annex I** to this Addendum sets out certain information regarding the Processing of the Customer Personal Data by Au10tix and/or any Sub-processors as required by Article 28(3) of the GDPR. Nothing in **Annex I** confers any right or imposes any obligation on any Party to this Addendum.

4. **Au10tix Personnel**

Au10tix will ensure that only those of the Au10tix employees who need to have access to the Customer Personal Data are granted access to such data and only for the purposes of the performance of the Services and ensure that all of the Au10tix personnel required to access the Customer Personal Data are informed of the confidential nature of the Customer Personal Data and are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. **Security**

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Au10tix will in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, as set forth in **Annex II**, of **Schedule 3**, which is attached and incorporated by reference to this Addendum. Customer is solely responsible for implementing appropriate internal measures for securing Customer Personal Data held and/or Processed by the Customer, including in connection with Customer's use of the Services, and for the secure transfer of Customer Personal Data to Au10tix.

6. **Sub processing**

6.1 Customer authorizes Au10tix to appoint (and permit each Sub-processor appointed in accordance with this section **Error! Reference source not found.** to appoint) Sub-processors in accordance with this section **Error! Reference source not found.** and any restrictions in the Agreement.

6.2 Au10tix may continue to use those Sub-processors already engaged by it at the date of this Addendum, as listed in **Annex II**.

6.3 Customer authorizes Au10tix to use additional Sub-processors, provided that Au10tix will notify Customer of the addition of any Sub-processors and give the Customer an opportunity to object in writing thereto, for reasonable and explained grounds, within fourteen (14) days of receiving such notice. If Customer timely sends Au10tix a written objection notice, the Parties will make a good-faith effort to resolve Customer's objection. In the absence of a resolution, Au10tix will make commercially reasonable efforts to provide Customer with the same level of Services, without using the additional Sub-processors to Process Customer Personal Data

6.4 With respect to each Sub-processors, Au10tix will ensure that such Sub-processors is required by written contract to abide by the same level of data protection and security as Au10tix under this Addendum, as applicable to such Sub-processors' Processing of Customer Personal Data.

7. **International Transfer of Personal Data**

7.1 Processing of Customer Personal Data pursuant to the Agreement will generally take place in data centers located within the EU, the United States or Japan (if Customer does not inform Au10tix in writing of its preferred data center location, the location will be determined by Au10tix). Customer Personal Data may also be Processed in the State of Israel.

7.2 Au10tix is allowed (and allowed to authorize its Sub-processors) to transfer Customer Personal Data outside of the EEA and UK in the following cases: **(a)** Customer Personal Data is transferred to the UK or a country within the European Union or to a country (such as the State of Israel) which is approved by the European Commission or by a UK Secretary of State as ensuring an adequate level of protection ("**Approved Jurisdictions**"); **(b)** subject to the entry into the Standard Contractual Clauses or any other lawful mechanism by the transferor and the

transferee with respect to the transfer of Customer Personal Data; or (c) if the transfer falls within a permitted derogation under the Data Protection Laws.

7.3 Transfer of GDPR-governed Customer Personal Data ("**EEA Transferred Data**") to a country which is not included in the Approved Jurisdictions, is made in accordance with the EU Standard Contractual Clauses ("**EU SCCs**"), pursuant to EU Commission Decision C(2021)3972, giving effect to the module specified in **Schedule 3**, which is attached and incorporated by reference to this Addendum, or, as required, in accordance with any successor thereof or an alternative lawful data transfer mechanism, and as follows:

7.3.1 In Clause 7, the optional docking clause will apply;

7.3.2 In Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processors changes will be as set out in Section 6 of this Addendum;

7.3.3 In Clause 11, the optional language will not apply;

7.3.4 In Clause 17, Option 1 will apply, and the EU SCCs will be governed by the Irish law;

7.3.5 In clause 18(b), disputes will be resolved before the courts of Ireland.

7.4 In accordance with Article 46 of the GDPR and the EU SCCs, and without prejudice to any provisions of this Addendum, Au10tix undertakes to implement the following organizational and technical safeguards, in addition to the safeguards mandated by the EU SCCs and in accordance with Clause 14(b)(iii) of the EU SCCs, to ensure the required adequate level of protection to the EEA Transferred Data:

7.4.1 Au10tix will implement and maintain the technical measures, as specified in **Annex II**, which is attached and incorporated by reference to this Addendum, with a purpose to protect the EEA Transferred Data from Processing for national security or other governmental purposes that goes beyond what is necessary and proportionate in a democratic society, considering the type of Processing activities under the Agreement and relevant circumstances;

7.4.2 For the purposes of safeguarding EEA Transferred Data when any government or regulatory agency requests access to such data in a country which is not included in the Approved Jurisdictions ("**Request**"), and unless required by a valid court order or if otherwise Au10tix may face criminal charges for failing to comply with orders or demands to disclose or otherwise provide access to EEA Transferred Data, or where the access is requested in the event of imminent threat to lives, Au10tix will:

7.4.2.1 not purposefully create 'back doors' or similar programming that could be used to access the EEA Transferred Data;

7.4.2.2 not provide the source code or encryption keys to any government agency for the purpose of accessing the EEA Transferred Data; and

7.4.2.3 upon Customer's written request, provide reasonable available information about the requests of access to Personal Data by government agencies that Au10tix has received in the six (6) months preceding to Customer's request.

7.4.3 If Au10tix receives a Request, Au10tix will notify Customer of such request to enable the Customer to take necessary actions, to communicate directly with the relevant agency and to respond to the Request. If Au10tix is prohibited by law to notify the Customer of the Request, Au10tix will make reasonable efforts to challenge such prohibition through judicial action or other means at Customer's expense and, to the extent possible, will provide only the minimum amount of information necessary.

7.5 Transfer of UK GDPR-governed Customer Personal Data ("**UK Transferred Data**") to a country which is not included in the Approved Jurisdictions, is either:

7.5.1 made in accordance with the EU Standard Contractual Clauses, pursuant to EU Commission Decision 2010/87/EU of 5 February 2010 ("**Previous EU SCCs**"), as officially published at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=EN, or other official publications of the European Union, *mutatis mutandis*, for as long as it is lawfully permitted to rely on in accordance with the UK GDPR, and on the following basis:

7.5.1.1 Appendix 1 to the Previous EU SCCs will be completed with the relevant information set out in Annex I to this Addendum;

7.5.1.2 Appendix 2 will be completed with the relevant information set out in Annex II to this Addendum; and

7.5.1.3 The optional illustrative indemnification Clause under Appendix 2 of the Previous EU SCCs will not apply.

or -

7.5.2 where Section 7.5.1 above does not apply, however the Parties are lawfully permitted to rely on the EU SCCs in relation to the UK Transferred Data subject to completion of a "UK Addendum to the EU Standard Contractual Clauses ("**UK Addendum**") issued by the UK Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 (officially published at: ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf), and officially published by the Information Commissioner's Office, then:

7.5.2.1 the EU SCCs giving effect to the module specified in **Schedule 3** which is attached and incorporated by reference to this Addendum, will also apply to UK Transferred Data, subject to Sections 7.3 and 7.4 above;

7.5.2.2 the UK Addendum will be deemed executed between the Parties, and the EU SCCs will be deemed amended as specified by the UK Addendum in relation to the UK Transferred Data.

or –

7.5.3 if neither Section 7.5.1 and 7.5.2 apply, then the Parties will cooperate in good faith to implement appropriate safeguards for transfers of UK Transferred Data, as required or permitted by the UK GDPR without undue delay.

8. **Data Subject Rights**

Taking into account the nature of the Processing, Au10tix will, at Customer's expense, provide reasonable assistance to Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligations to respond to and comply with requests to exercise Data Subject rights under the applicable Data Protection Laws.

9. **Personal Data Breach**

Taking into account the nature of Processing and the information available to Au10tix, it will, at Customer's expense, notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data which Au10tix, or any of its Sub-processors, Process, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects or a Supervisory Authority of the Personal Data Breach. Such notice shall include, at the time of notification or without further delay after notification, with respect to Customer Personal Data, details of the nature of the breach and number of records affected, the category and approximate number of affected Data Subjects,

anticipated consequences of the breach and any actual or proposed remedies for mitigating the possible adverse effects of the breach.

10. **Data Protection Impact Assessment and Prior Consultation**

Au10tix will, at Customer's expense, provide reasonable assistance to Customer with data protection impact assessments, and prior consultations with Supervisory Authorities, which Customer reasonably considers to be required by Article 35 or 36 of the GDPR, in each case solely in relation to Processing of Customer Personal Data in accordance with the Agreement and this Addendum by, and taking into account the nature of the Processing and information available to Au10tix.

11. **Deletion of Customer Personal Data**

11.1 Au10tix will delete all Customer Personal Data within reasonable time after the termination of the Agreement, including by de-identifying thereof. Customer shall have a right, throughout the term of the Agreement, to instruct Au10tix in writing to delete any part of the Customer Personal Data.

11.2 Notwithstanding Section 11.1, Au10tix may retain Customer Personal Data as necessary in connection with its routine backup and archiving procedures, to ensure compliance with its legal obligations and its continuing obligations under applicable laws, to use such data to protect Au10tix, its affiliates or any person on their behalf in court and administrative proceedings and to the extent and for such period as required by a subpoena or other judicial or administrative order, or if otherwise required by law. Au10tix will ensure the confidentiality of all such Customer Personal Data and will ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

12. **Audit rights**

12.1 Subject to section 12.2 below, Au10tix will make reasonable efforts to make available to Customer on request information necessary to demonstrate compliance with this Addendum (to the extent required by the applicable Data Protection Laws).

12.2 During the term of the Agreement, Au10tix will Allow Customer to audit Au10tix's compliance with its obligations under Sections 2-10 of this Addendum up to once per each calendar year ("**Audit**"), provided, however, that any such Audit is subject to the following cumulative conditions:

12.2.1 the Audit will be pre-scheduled in writing with Au10tix, at least thirty (30) days in advance and will be conducted during normal business hours only;

12.2.2 Customer may only mandate an auditor for the purposes of conducting an Audit on its behalf pursuant to this Section 12 if the auditor is agreed to by Au10tix;

12.2.3 All personnel participating in the Audit, whether employed or contracted by Customer and/or third-party auditor ("**Audit Personnel**"), will execute Au10tix's standard non-disclosure and non-competition undertakings prior to the initiation of the Audit;

12.2.4 The Audit Personnel will not have access to non-Customer data. Customer will take all necessary measures to verify that Audit Personnel do not disclose or compromise the confidentiality and security of data on Au10tix's information and network systems;

12.2.5 Customer will make sure that the Audit will not interfere with, or damage, to Au10tix's business activities and information and network systems;

12.2.6 Customer will bear all costs and assume responsibility and liability for the Audit and for any failures or damage caused as a result thereof;

12.2.7 The Customer will first deliver a draft report of the Audit to Au10tix and allow Au10tix reasonable time and no less than ten (10) business days, to review and respond to the Audit's findings;

12.2.8 Customer will receive only the Audit report, with Au10tix's comments, without any Au10tix's 'raw data' materials. Customer will keep the Audit results in strict confidentiality, will use them solely for the specific purposes of the Audit under this

section, will not use the results for any other purpose, or share them with any third party, without Au10tix's prior explicit written confirmation; If Customer is required to disclose the Audit results to a competent authority, Customer will first provide Au10tix with a prior written notice, explaining the details and necessity of the disclosure, and an opportunity to object, and will provide Au10tix with assistance to prevent the disclosure thereof, in accordance with applicable law;

12.2.9 As soon as the purpose of the Audit is completed, Customer will permanently and completely dispose of all copies of the Audit report; and,

12.2.10 Au10tix will inform Customer if, in its opinion, an instruction in connection with this Section 12 infringes applicable laws.

12.3 Au10tix may satisfy the Audit obligation under Section 12.2 above by providing Customer with attestations, certifications and summaries of audit reports conducted by accredited third party auditors.

13. Term

This Addendum will commence on the same date that the Agreement is effective, or as otherwise provided explicitly under this Addendum, and will continue until the Agreement expires or is terminated, pursuant to the terms therein.

14. Dispute Resolution

Each Party will create an escalation process and provide a written copy to the other Party within five (5) business days of any dispute arising out of or relating to this Addendum. The escalation process will be used to address disputed issues related to the performance of this Addendum, including but not limited to technical problems. The Parties agree to communicate regularly about any open issues or process problems that require prompt and accurate resolution as set forth in their respective escalation process documentation. The Parties will attempt in good faith to resolve any dispute arising out of or relating to this Addendum, before and as a prior condition for commencing legal proceedings of any kind, first as set forth above in the escalation process and next by negotiation between executives who have authority to settle the controversy and who at a higher level of management than the persons with direct responsibility for administration of this Addendum. Any Party may give the other Party written notice of any dispute not resolved in the normal course of business. Within two (2) business days after delivery of the notice, the receiving Party shall submit to the other a written response. The notice and the response will include (a) a statement of each Party's position and a summary of arguments supporting that position and (b) the name and title of the executive who will represent that Party and of any other person who will accompany the executive. Within five (5) business days after delivery of the disputing Party's notice, the executives of both Parties shall meet at a mutually acceptable time and place, including telephonically, and thereafter as often as they reasonably deem necessary, to attempt to resolve the dispute. All reasonable requests for information made by one Party to the other will be honored. All negotiations pursuant to this clause are confidential and will be treated as compromise and settlement negotiations for purposes of applicable rules of evidence. The dispute resolution process under this section 14 must be exercised as a pre-condition for initiating legal or administrative proceedings by any of the Parties.

15. General Terms

Disclosure to competent authorities

15.1 To the extent required by applicable law, Au10tix may retain or disclose Customer Personal Data if required by a subpoena or other judicial or administrative order, or if otherwise required by law, or if Au10tix deems the disclosure necessary to protect the safety and rights of any person, or the general public, provided that Au10tix will, prior to such disclosure and to the extent permitted by applicable law, notify Customer and provide Customer an opportunity to object to such disclosure.

Order of precedence

15.2 With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the Parties, the provisions of this Addendum shall prevail. In the event of inconsistencies between the provisions of this Addendum and any Annex, the provisions of the Annex shall prevail.

Severance

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

15.4 Any claims brought under this Addendum will be subject to the terms and conditions of the Agreement, including the exclusions and limitations set forth in the Agreement. Any alteration or modification of this Addendum is not valid unless made in writing and executed by duly authorized personnel of both Parties.

15.5 This Addendum may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. In the event that a Party's signature is delivered by facsimile transmission or by e-mail delivery of a ".pdf" format data file, such signature shall create a valid and binding obligation of such Party with the same force and effect as if such facsimile or ".pdf" signature page were an original thereof.

Anonymized and Aggregated Data

15.6 Au10tix may Porecess data based on extracts of Customer Personal Data on an aggregated and non-identifiable form, for Au10tix's legitimate business purposes, including for testing, development, controls, and operations of the Services, and may share and retain such data at Au10tix's discretion, provided that such data cannot reasonably identify a Data Subject.

SCHEDULE 1
DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This **Schedule 1** includes certain details of the Processing of Customer Personal Data pursuant to Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data
The subject matter of the Processing of Customer Personal Data is set out in the Agreement between the Parties and the duration thereof is for the term of the Agreement.

The nature and purpose of the Processing of Customer Personal Data
Au10tix and any Sub-processors may Process Customer Personal Data for the purpose of providing the Services (and in particular, ID document authentication and onboarding services, as well as customer support services) to the Customer, including by: **(a)** examining irregular/suspicious attributes of government-issued IDs or passports and/or information contained therein ("**ID Data**") and providing the Customer with an analysis thereof; **(b)** providing technical and other support to Customer with respect to the Services; **(c)** conducting quality assurance checks and sanity checks; **(d)** maintaining and improving the Services and the technology used therefor; **(e)** complying with Customer's documented written instructions; or **(f)** complying with applicable law.

Serial Fraud Monitor (FAKA - INSTINCT) Risk Analytics

If the Services under the applicable Purchase Order include SFM Risk Analytics, Au10tix will retain and Process encrypted signals containing portions of Customer Personal Data for analysis purposes, fraud prevention, reducing business risks, and alerting customers against different types of fraud or potential misuse of government-issued identification cards or passports. If Au10tix's analyses raise reasonable concern for fraud and/or misuse of a certain form of identification, Au10tix also may communicate the existence of such concern (without disclosing the form of identification or personal data contained therein) to other customers that may ask Au10tix to analyze that same form of identification, without disclosing or sharing Customer Personal Data or any portion thereof, and solely for the limited purposes specified herein, warn and/or alert other customers regarding such suspected fraud and/or misuse of government-issued identification card or passport. With regards to any retained Customer Personal Data Au10tix applies data minimization principles, and has implemented and maintains appropriate technical and organizational safeguards, such as **(a)** the encryption of Customer Personal Data; **(b)** the ability to reasonably ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. At any time Au10tix shall promptly and with no undue delay delete and/or permanently destroy Customer Personal Data in its possession, upon the earlier of: **(i)** Customer's written request; and **(ii)** the termination or expiration date of the Agreement. As explained in Section 11 of this Addendum, the Customer can, throughout the term of the Agreement, instruct Au10tix in writing to delete any part of the Customer's Personal Data.

The types of Customer Personal Data to be Processed
Customer Personal Data typically includes some or all of the following: ID Data, name, legal name, user name, email, location, geo-location of a photo, physical address, gender, date of birth, nationality, names of parents, photo, place and date of issuance government-issued identification card or passport and all other information contained therein, and metadata derived from electronic communications (device ID, Customer ID, OS Version, device model, application bundle ID and location data).

The categories of Data Subject to whom the Customer's Personal Data relates

Data Subjects typically include Customer personnel, customers of Customer, and users of Customer's products or services, all determined solely and independently by Customer.

The obligations and rights of the parties
The obligations and rights of the Controller and Processor are set out in this Addendum.

SCHEDULE 2

AUTHORIZED SUB-PROCESSORS

The list of Sub-processors is available at https://www.au10tix.com/downloads/

SCHEDULE 3

EU Standard Contractual Clauses

ANNEX to the COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as officially published at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj or other official publications of the European Union as updated from time to time:

☑ *MODULE TWO: Transfer controller to processor.*

ANNEX I
DETAILS OF THE PROCESSING ACTIVITIES

A. **LIST OF PARTIES**

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

Customer's details as indicated in the applicable form.

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

1. Name: AU10TIX Ltd.
Address: 5B, Hanagar St. Hod Hasharon, Israel.
Contact person's name, position and contact details: DPO@au10tix.com
Activities relevant to the data transferred under these Clauses: As described in **Schedule 1** of the Addendum.
Signature and date: as the date of the signature of this agreement.
Role: Processor

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred:
As mentioned under **Schedule 1**.

Categories of personal data transferred:
As mentioned under **Schedule 1**.

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:
As mentioned under **Schedule 1**.

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

Continuous.

Nature of the processing:

As mentioned under **Schedule 1**, all operations such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means), etc.

Purpose(s) of the data transfer and further processing:

The provision of the Service in accordance with the Agreement.

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

Personal Data will be retained during the term of the Agreement and will be deleted in accordance with the terms therein.

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

The subject matter and the nature of the Processing is as mentioned under **Schedule 1**, and the duration of the Processing is the term of the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Where the data exporter is established in an EU Member State - the supervisory authority of such EU Member State 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 the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) - the supervisory authority of the Member State in which the representative is established 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 the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) - the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses, shall act as competent supervisory authority.

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

1. **General**

Au10tix undertakes to fulfill Customer's requirements with regard to information security as specified in this Addendum and this Annex, and to take strict cautionary measures, and carry out all that is required in all aspects, for the purpose of maintaining the security of the Personal Data in its possession, as described in this Addendum and in accordance with Data Protection Laws.

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

External Attack Surface. Au10tix employs multiple layers of network devices and intrusion detection to protect its external attack surface. Au10tix considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Au10tix undertakes that it will employ intrusion detection, which is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Au10tix's intrusion detection involves: (a) tightly controlling the size and make-up of Au10tix's attack surface through preventative measures; (b) employing intelligent detection controls at data entry points; and (c) employing technologies that automatically remedy certain dangerous situations.

Incident Response. Au10tix monitors a variety of communication channels for security incidents, and Au10tix's security personnel will react promptly, not later than the time stated in the Agreement or the Addendum, to known incidents.

3. **Measures for the protection of data during transmission and storage**

Encryption in transit. Au10tix should use industry-standard such as SSL/TLS between endpoints/partners and its data centers.

Encryption at rest. Personal Data should be encrypted according to industry-standard encryption algorithms.

4. **Measures for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing and measures for ensuring system configuration, including default configuration.**

Au10tix undertakes to secure its information systems as follows:

Risk Assessments and Penetration Tests. To carry out periodic reviews, vulnerability assessments, penetration tests and risk assessments for the information systems on which the Personal Data is stored from time to time and as reasonably required, and in any case at least every 12 months, and in case of critical finding it will be addressed immediately and Au10tix will take all of the required measures for the purpose of correcting the deficiencies that are discovered as a result of such assessments and checks. In case of medium and lower findings, Au10tix will decide the required action based on a risk-based approach process. Au10tix will enable the Customer to conduct, at its own expense, independent penetration tests against Au10tix's application/service/infrastructure. Au10tix commits to cooperate with Customer's security personnel to mitigate any critical or high severity finding (as defined by Customer) as a result of these tests within an agreeable timeframe.

Information Security Technologies. To have suitable information security technologies and measures implemented for the organizational network that will prevent unauthorized access to Personal Data, and to protect Au10tix's information systems, including workstations, servers, network systems, end-user equipment, and portable equipment, through industry best-practice information security technologies for the prevention of unauthorized access of information and information systems, including monitoring systems, documentation, and alerts on unauthorized access attempts.

Separation of Systems. To store the Personal Data of the Customer only on Au10tix's designated central systems and not on personal workstations.

Security Updates. To regularly update the security systems connected to the Personal Data and in accordance with the manufacturer's guidelines and recommendations. Critical updates (patches) should be applied no later than one week after they become aware to Au10tix.

Encryption of Data in Public Networks. Not to permit access to the database infrastructure from the internet, and not to transmit the Personal Data over the internet or other public networks, except if the Personal Data is encrypted in an industry best-practice method of encryption and the user identifies him/herself through means that are under his/her exclusive control.

Data Isolation. To logically isolate Personal Data to prevent isolation failures.

5. **Measures for user identification and authorization**

Access Control and Privilege Management. Access to Personal Data must be done via secure private network (VPN), from a workstation managed by Au10tix and by using at least unique username, unique complex password and a multi-factor authentication. Access to the Personal Data must be properly logged and monitored (audit trail).

Internal Data Access Processes and Policies. Au10tix's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to Process Personal Data. Au10tix aims to design its systems to: **(a)** only allow authorized persons to access Personal Data they are authorized to access; and **(b)** ensure that Personal Data cannot be read, copied, altered or removed without authorization during Processing, use and after recording. The systems are designed to detect any inappropriate access.

Personnel Security. Au10tix personnel are required to conduct themselves in a manner consistent with its guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Au10tix conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Au10tix's confidentiality and privacy policies. Personnel handling Customer Personal Data are required to complete additional requirements appropriate to their role. Au10tix's personnel will not process Customer Personal Data without authorization.

Au10tix has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Au10tix is responsible for the ongoing monitoring of Au10tix's security infrastructure and responding to security incidents.

6. **Measures for ensuring physical security of locations at which Personal Data are processed**. Au10tix undertakes to take physical security measures as follows: **(a)** To store written material and portable devices that contain Personal Data only in a safe box or in locked cabinets located at Au10tix's offices; **(b)** to take due care that Au10tix's offices and the offices of the contracted Sub-processors, if such are employed by Au10tix for the performance of the Agreement, are equipped with a suitable alarm protection system against infiltrations; **(c)** to only allow physical access to Au10tix grounds to authorized personnel; **(d)** to protect Au10tix's server rooms and central information systems with physical methods and to carry out computerized auditing and documentation of the access or the access attempts to these rooms, including the name of the person requesting access, and the date and time of the access attempt; **(e)** in the case of the provision of the Services on Customer's grounds, to maintain the confidentiality of the authorization password (if such is provided to Au10tix's employees), to lock the screens and the workstations every time the Customer's employees leave the workstations and to shut down computers at the end of the work day; **(f)** to strictly implement a "clean desk" policy at the end of the workday.

7. **Business continuity and disaster recovery plans (or measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical and technical incident)**. AU10TIX Services will have defined, documented, maintained and annually validated business continuity and disaster recovery plans consistent with industry standard practices.

8. **Measures for ensuring events logging**. Access will be monitored and logged.

ANNEX III – LIST OF SUB-PROCESSORS

As detailed in **Schedule 2** of the Addendum.