Data Processing Agreement

This Data Processing Agreement (the "**DPA**") is effective _____ ("**Effective Date**") and is made by and between Immuta Inc., ("**Immuta**") and _____ ("**Licensee**") and is subject to the _____ Agreement effective _____ (the "**Agreement**").

This DPA is incorporated into the Agreement between Immuta and Licensee and applies to Immuta's Processing of Personal Data in connection with Immuta's provision of the Services (as defined in the Agreement) to Licensee. In the event of any inconsistency between the DPA and the Agreement as to Immuta's Processing of Personal Data, the DPA shall control.

---

1. DEFINITIONS

1.1 In this DPA, the terms "**Personal Data**", "**Controller**", "**Processor**", "**Data Subject**", "**Process**" and "**Supervisory Authority**" shall have the same meaning as set out in applicable Data Protection Laws with the same or equivalent terms, and the following words and expressions shall have the following meanings unless the context otherwise requires:

1.2 "**Licensee Personal Data**" means any Personal Data that Immuta Processes on behalf of Licensee in the course of utilizing the Services as a Processor, which, for clarity, excludes Usage Data.

1.3 "**Data Protection Laws**" means all applicable laws, rules and regulations relating to the Processing of Personal Data as amended, repealed, consolidated or replaced from time to time.

1.4 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Licensee Personal Data by Immuta that compromises the security, confidentiality or integrity of such Licensee Personal Data.

1.5 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

1.6 "**Subprocessor**" means any Processor engaged by Immuta to Process Licensee Personal Data on Immuta's behalf.

1.7 "**Third Country**" means any destination country outside of a source country in which the Data Protection Laws restrict transfers of Personal Data to such other destination countries, except where the Data Protection Laws and applicable regulatory authorities of the source country adopted an adequacy decision regarding the Data Protection Laws of the destination country such that transfers of Personal Data to that destination country are not restricted. For purposes of this DPA, the United States is a Third Country.

1.8 "**UK Addendum**" means United Kingdom ("UK") Information Commissioner's ("ICO") International Data Transfer Addendum to the EU Commission Standard Contractual Clauses Version B1.0 in force 21 March 2022.

1.9 “**Usage Data**” means information and data relating to the manner in which Licensee uses the Service.

Capitalized terms used in this DPA and not defined above shall have the meaning set forth in the Agreement.

2. DATA PROCESSING

2.1 Immuta will only Process Licensee Personal Data in accordance with the Agreement (including any order form), and Licensee’s written instructions, to the extent necessary to provide the Services to Licensee, including with respect to transfers of Licensee Personal Data, unless Processing is required by other applicable laws, in which case Immuta shall, to the extent permitted by applicable law, inform Licensee of that legal requirement before so Processing that Licensee Personal Data. Immuta shall not Process Licensee Personal Data outside of the direct business relationship between Licensee and Immuta. Immuta shall not ‘sell’ or ‘share’ (as such terms may be specifically defined in applicable Data Protection Laws) Licensee Personal Data. The Agreement (including any order form) and the DPA shall be Licensee’s complete and final instructions to Immuta in relation to the Processing of Licensee Personal Data. Processing outside the scope of the foregoing will require prior written agreement between Licensee and Immuta on additional instructions for Processing and may be subject to additional fees.

2.2 Licensee shall provide all applicable notices to Data Subjects required under applicable Data Protection Laws for the lawful Processing of Licensee Personal Data by Immuta in accordance with the Agreement. Licensee shall obtain and maintain throughout the term of the Agreement any required consents and/or authorizations related to its provision of, and Immuta’s processing of, Licensee Personal Data as part of the Services. If Licensee is not required by Data Protection Laws to obtain and maintain valid consent from Data Subjects, Licensee will otherwise obtain and maintain a valid legal basis in accordance with Data Protection Laws to Process Licensee Personal Data and for providing such data to Immuta for Processing under the Agreement.

2.3 For the avoidance of doubt, Licensee’s instructions for the processing of Licensee Personal Data shall comply with the Data Protection Laws. Licensee acknowledges that Immuta is reliant on Licensee for direction as to the extent to which Immuta is entitled to use and Process Licensee Personal Data. Consequently, Immuta will not be liable for any claim brought against Immuta by a Data Subject arising from any act or omission by Immuta to the extent that such act or omission resulted from Licensee’s instructions or Licensee’s use of the Services.

2.4 Unless otherwise expressly permitted by Immuta, Licensee Personal Data shall not include any sensitive or special data that imposes specific data security or data protection obligations on Immuta in addition to or different from those specified in Agreement or which are not provided as part of the Services.

2.5 If applicable Data Protection Laws recognize the roles of Controller and Processor as applied to Licensee Personal Data then, as between Licensee and Immuta, Licensee acts as Controller and Immuta acts as a Processor (or Subprocessor, as the case may be) of Licensee Personal Data. When Immuta processes Personal Data as a Controller, for example when processing personal data of Licensee’s authorized representatives or Authorized Users when

Licensee purchases, renews or cancels its subscription or when processing Usage Data, Immuta will comply with its obligations under Data Protection Law, including, as required, providing Data Subjects with a privacy statement or privacy notice at the time of collection or before any Processing takes place. By entering into the Agreement, Licensee agrees that Personal Data will be transferred to the United States of America or other countries as set forth in Schedule 1 Annex III for purposes such as providing the Services as a Processor, account registration, administration, billing, communication with customers, direct marketing, security, license compliance and fraud prevention, user experience optimization, product and service improvements.

2.6 As required by applicable Data Protection Laws, if Immuta believes any Licensee instructions to Process Licensee Personal Data will violate applicable Data Protection Laws, or if applicable Data Protection Laws require Immuta to process Licensee Personal Data relating to data subjects in a way that does not comply with Licensee's documented instructions, Immuta shall notify Licensee in writing, unless applicable Data Protection Laws prohibit such notification, provided Immuta is not responsible for performing legal research or providing legal advice to Licensee.

2.7 Immuta shall Process Licensee Personal Data for the duration of the provision of Services in accordance with the Agreement and thereafter only as set forth in the Agreement and this DPA.

2.8 Each party will comply with Data Protection Laws applicable to such party in connection with the Agreement and this DPA.

3. SUBPROCESSORS

3.1 Consent to Subprocessor Engagement. Licensee generally authorizes the engagement of third parties as Subprocessors provided such engagement complies with this Section 3. For the avoidance of doubt, this authorization constitutes Licensee's prior written consent to the subprocessing of Licensee Personal Data for purposes of Clause 9, Option 2 of the Standard Contractual Clauses and any similar requirements of other data transfer mechanisms.

3.2 Information about Subprocessors. A current list of Subprocessors is available here ("Subprocessor List") and may be updated by Immuta from time to time in accordance with this DPA. Immuta will provide notice of additions to the Subprocessor List via email.

3.3 Requirements for Subprocessor Engagement. When engaging any Subprocessor, Immuta will:

(a) execute with Subprocessors a written agreement providing:

(i) the Subprocessor only Processes Licensee Personal Data only to the extent required to perform the obligations subcontracted to it and does so in accordance with the Agreement and this DPA; and

(ii) the Subprocessor utilizes substantially the same level of data protection and security with regard to its Processing of Licensee Personal Data as described in this DPA.

(b) be responsible for the Subprocessor's violations of this DPA or Data Protection Laws in relation to the services such Subprocessor provides to Immuta to the extent Immuta would be liable for the same violations under the terms of the Agreement.

3.4 Opportunity to Object to Subprocessor Changes**.** Licensee may, on reasonable and objective grounds, object to Immuta's use of a new Subprocessor by providing Immuta with written notice within ten (10) days after Immuta has provided notice to Licensee as described herein with documentary evidence that reasonably shows that the Subprocessor does not or cannot comply with the requirements in this DPA or Data Protection Laws ("Objection"). In the event of an Objection, Licensee and Immuta will work together in good faith to find a mutually acceptable resolution to address such Objection, including but not limited to reviewing additional documentation supporting the Subprocessor's compliance with the DPA or Data Protection Laws. To the extent Licensee and Immuta do not reach a mutually acceptable resolution within a reasonable timeframe, Immuta will use reasonable endeavors to make available to Licensee a change in the Services or will recommend a commercially reasonable change to the Services to prevent the applicable Subprocessor from Processing Licensee Personal Data. If Immuta is unable to make available such a change within a reasonable period of time, which shall not exceed thirty (30) days, Licensee shall, as its sole remedy, have the right to terminate the relevant Services (i) in accordance with the termination provisions in the Agreement; (ii) without liability to Licensee or Immuta, and (iii) without relieving Licensee from its payment obligations under the Agreement up to the date of termination.

4. INTERNATIONAL TRANSFERS

4.1 In accordance with Licensee's instructions under Section 2, Immuta may Process Licensee Personal Data on a global basis as necessary to provide the Services, including for IT security purposes, maintenance and provision of the Services and related infrastructure, technical support, and change management.

4.2 To the extent that the Processing of Licensee Personal Data by Immuta involves the transfer of such Licensee Personal Data from a country whose Data Protection Laws restrict the transfer of Personal Data to Third Countries, then such transfers shall be subject to the protections and provisions of the Standard Contractual Clauses (the Appendix for which is attached to this DPA in Schedule 1), the UK Addendum for transfers from the UK to Third Countries, or other binding and appropriate transfer mechanisms that provide an adequate level of protection in compliance with Data Protection Laws. For purposes of this Section 4, transfers to the United States shall be carried out under the SCCs and UK Addendum, as applicable.

4.3 Licensee shall be deemed to have signed the SCC in Schedule 1, Annex I in its capacity of "data exporter" and Immuta in its capacity as "data importer." Module One of the SCCs shall apply when Licensee and Immuta both act as Controller of the Personal Data. Module Two shall apply when Licensee is Controller of the Licensee Personal Data and Immuta is Processor of such data. Module Three shall apply when Licensee is a Processor of the Licensee Personal Data on behalf of its customer and Immuta is a subprocessor of such data. If Module Three applies, Licensee hereby notifies Immuta that it is a Processor and the instructions shall be as set forth in this DPA. For purposes of Clauses 17 and 18 of the SCCs, the Parties select The Netherlands. Clause 7 is omitted. In Clause 11(a), the optional provision shall not apply. Additional provisions applicable to customer Personal Data transferred pursuant to SCC are set forth in Schedule 2. To the extent such a transfer includes Personal Data subject to Data

Protection Laws of Switzerland, the Standard Contractual Clauses shall be adapted to use for Switzerland (where the Swiss Federal Act on Data Protection shall apply as the applicable Data Protection Law, Clauses 17 and 18 of the SCCs shall refer to Switzerland, and Data Subjects in Switzerland shall be able to avail themselves of any rights conferred by the Standard Contractual Clauses).

4.4 If the UK Addendum applies, then:

(a) Table 1 of the UK Addendum is completed with the Parties's details and Key Contacts of Licensee (as data exporter) and Immuta (as data importer), as provided above. The "Start date" is the Effective Date or other similar date of the Agreement.

(b) Table 2 of the UK Addendum is completed by selecting "the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum".

(c) For the purposes of Table 2 and Table 3 of the UK Addendum, the "Approved EU SCCs" are completed with the Modules, selections, and details set forth above.

(d) Table 4 of the UK Addendum is completed by selecting "neither party".

4.5 The SCC, or UK Addendum, as applicable, will cease to apply if Immuta has implemented an alternative recognized compliance mechanism for the lawful transfer of personal data in accordance with applicable Data Protection Laws.

4.6 In the event of any conflict between any terms in the SCC or UK Addendum, as applicable, and the DPA, the SCC or UK Addendum, as applicable, shall prevail to the extent of the conflict.

5. DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS

5.1 Immuta Security Obligations**.** 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, Immuta shall implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk of the Processing, including the measures set out in Schedule 1. Immuta may update its security practices from time to time but will not materially decrease the overall security of the Services during the term of the Agreement. Such measures shall include processes for regularly testing, assessing, and evaluating the effectiveness of the measures.

5.2 Security Audits.

(a) Immuta will, upon Licensee's written request, verify its compliance with its obligations in this DPA by first providing to Licensee for its review documentation regarding the same and, if such documentation is not reasonably sufficient to address Licensee's inquiries, participate in and contribute to audits as set forth below.

(b) Licensee may, upon at least 30 days' advance written notice and at reasonable times, audit (either by itself or using independent third-party auditors) Immuta's compliance with the security measures set out in this DPA solely for the purpose of confirming Immuta's compliance with its obligations under this DPA. Immuta shall reasonably assist with any audits

conducted in accordance with this Section 5.2. Such audits may be carried out once per year, or more often if required by Data Protection Law or Licensee's applicable Supervisory Authority.

(c) Any third party engaged by Licensee to conduct an audit must be pre-approved by Immuta (such approval not to be unreasonably withheld) and sign Immuta's confidentiality agreement. Licensee must provide Immuta with a proposed audit plan at least two weeks in advance of the audit, after which Licensee and Immuta shall discuss in good faith and finalize the audit plan prior to commencement of audit activities.

(d) Audits may be conducted only during regular business hours, in accordance with the finalized audit plan and Immuta's security and other policies and may not unreasonably interfere with Immuta's regular business activities. Immuta is not required to grant access to its premises or systems for the purposes of such an audit to any individual unless they produce reasonable evidence of identity and authority. Licensee shall reimburse Immuta for any costs or expenses incurred by Immuta in connection with the Audit or with granting access to its data processing facilities.

(e) Information obtained or results produced in connection with an audit are Immuta confidential information and may only be used by Licensee to confirm compliance with this DPA and for complying with its requirements under Data Protection Laws.

(f) In lieu of Licensee auditing a Subprocessor, Licensee may request that Immuta audit a Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist Licensee in obtaining a third-party audit report concerning the Subprocessor's operations) to verify compliance with the Subprocessor's obligations.

(g) Without prejudice to the rights granted in Section (b) above, if the requested audit scope is addressed in a SOC, ISO, or similar audit report or attestation letter issued by a qualified third party auditor within the prior twelve months and Immuta provides such report or attestation letter to Licensee confirming there are no known material changes in the controls audited, Licensee agree to accept the findings presented in the third party audit report or attestation letter in lieu of requesting an audit of the same controls covered by the report.

5.3 Upon Licensee's written request, Immuta shall make available all information reasonably necessary to demonstrate compliance with this DPA as required by Data Protection Laws.

5.4 Personal Data Breach Notification.

(a) If Immuta or any Subprocessor becomes aware of and determines a Personal Data Breach has occurred, Immuta will:

(i) notify Licensee of the Personal Data Breach without undue delay and, in any case, within seventy-two (72) hours after such determination, at the contact information on file, where such notification shall describe (1) the nature of the Personal Data Breach 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 reasonably anticipated consequence of the Personal Data Breach; (3) measures taken to mitigate any possible adverse effects; and (4) other information concerning the Personal Data Breach reasonably known or available to Immuta that

Licensee is required to disclose to a Supervisory Authority or Data Subjects under Data Protection Laws; and

(ii) investigate the Personal Data Breach and provide such reasonable assistance to the Client (and any law enforcement or regulatory official) as required to investigate the Personal Data Breach.

5.5 Except as required by applicable Data Protection Laws, the obligations set out in Section 5.4 shall not apply to Personal Data Breaches caused by Licensee.

5.6 Immuta's contact point for additional details regarding a Personal Data Breach is privacy@immuta.com. Immuta's provision of any notification of a Personal Data Breach shall not constitute an admission of fault.

5.7 Licensee is solely responsible for fulfilling any Personal Data Breach notification obligations applicable to Licensee. Licensee and Immuta shall work together in good faith within the timeframes for Licensee to provide Personal Data Breach notifications in accordance with Data Protection Laws to finalize the content of any notifications to Data Subjects or Supervisory Authorities, as required by Data Protection Laws. Immuta's prior written approval shall be required for any statements regarding, or references to, Immuta made by Licensee in any such notifications.

5.8 Immuta shall treat Licensee Personal Data as the Confidential Information of Licensee, and shall put procedures in place to ensure that any employees or other personnel with access to Licensee Personal Data have committed themselves to confidentiality of Licensee Personal Data or are under an appropriate statutory obligation of confidentiality and do not Process such Licensee Personal Data other than in accordance with this DPA.

5.9 Licensee is responsible for security relating to its environment and databases and security relating its configuration of the Services. This includes implementing and managing procedural, technical, and administrative safeguards on its software and networks sufficient to: (a) ensure the confidentiality, security, integrity, and privacy of Licensee Personal Data in transit, at rest, and in storage; (b) protect against any anticipated threats or hazards to the security and integrity of Licensee Personal Data; and (c) protect against any unauthorized processing, loss, use, disclosure or acquisition of or access to Licensee Personal Data. Notwithstanding any other provision of this DPA, the Agreement or any other agreement related to the Services, Immuta will have no obligations or liability as to any breach or loss resulting from: (x) Licensee's environment, databases, systems or software, or (y) Licensee's security configuration or administration of the Services.

6. ACCESS REQUESTS AND DATA SUBJECT RIGHTS

6.1 Save as required (or where prohibited) under applicable law, Immuta shall promptly notify Licensee of any request received by Immuta or any Subprocessor from a Data Subject in respect of their Personal Data included in Licensee Personal Data ("Data Subject Request") and shall not respond to the Data Subject Request where the Data Subject identifies Licensee as its Controller. If a Data Subject does not identify a Controller, Immuta will instruct the Data Subject to identify and contact the relevant Controller.

6.2 Where applicable, and taking into account the nature of the Processing, Immuta shall use reasonable endeavors to assist Licensee by implementing appropriate technical and

organizational measures, insofar as this is possible, for the fulfillment of Licensee's obligation to respond to Data Subject Requests as required by Data Protection Laws. In order to receive such assistance, Licensee shall utilize any tools provided by Immuta including those providing Licensee with the ability to correct, delete, block, access or copy the Personal Data of a Data Subject. If such functionality or other tools are not available, Licensee may contact privacy@immuta.com requesting assistance and clearly stating the nature of the Data Subject Request.

7. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

7.1 To the extent required under applicable Data Protection Laws, Immuta shall provide reasonable assistance to Licensee with any data protection impact assessments and with any prior consultations to any Supervisory Authority of Licensee, in each case solely in relation to Processing of Licensee Personal Data and taking into account the nature of the Processing and information available to Immuta.

7.2 Such cooperation and assistance are provided to the extent Licensee does not otherwise have access to the relevant information, and to the extent such information is available to Immuta. Immuta may fulfill its above obligations by providing Licensee with documentation regarding its Processing operations.

8. RETRIEVAL AND DELETION OF PERSONAL DATA

8.1 After (i) cessation of Processing of Licensee Personal Data by Immuta on Licensee's written request or (ii) termination or expiration of the Agreement, except as otherwise permitted by applicable Data Protection Laws, Immuta shall retain Licensee Personal Data then available in the Services in electronic format for ninety (90) days ("Retrieval Period") and thereafter delete and use all reasonable efforts to procure the deletion of all other copies of Licensee Personal Data Processed by Immuta or any Subprocessors, and where deletion is not possible, sufficiently de-identify Licensee Personal Data such that it is no longer Personal Data.

8.2 Licensee may access Licensee Personal Data during the term of the Agreement and the Retrieval Period.

8.3 Immuta may retain Licensee Personal Data to the extent required by applicable Data Protection Laws, and only to the extent and for such period as required by applicable Data Protection Laws, and always provided that Immuta shall ensure the confidentiality of all such Licensee Personal Data and shall ensure that such Licensee Personal Data is only Processed as necessary for the purpose(s) specified in the applicable Data Protection Laws requiring its storage and for no other purpose.

9. GENERAL

9.1 With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including but not limited to the Agreement, the provisions of this DPA shall prevail with regard to the parties' data protection obligations for Licensee Personal Data of a Data Subject.

9.2 Immuta may share and disclose Licensee Personal Data and other data of Licensee in connection with, or during the negotiation of, any merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of Immuta's business by or to another

company, including the transfer of contact information and data of customers, partners and end users.

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

IN WITNESS WHEREOF, the Parties' authorized representatives have executed this DPA as of the Effective Date.

CUSTOMER: _____		**IMMUTA, INC.**	
Signed:	_____	Signed:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

SCHEDULE 1

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX I

ANNEX I.A – LIST OF PARTIES

Data exporter(s): identity of the Licensee as set forth in the preamble of the Agreement

Contact person's name, position and contact details: …
Activities relevant to the data transferred under these Clauses: …
Signature and date: …
Role (controller/processor): Controller

Data importer(s):

Name: Immuta, Inc.
Address: 25 Thomson Place, 4th Floor, Boston MA 02110, USA
Contact person's name, position and contact details: …
Activities relevant to the data transferred under these Clauses: Performing the obligations of Immuta under the Agreement and complying with its legal and judicial obligations
Signature and date: …
Role (controller/processor): Processor and Controller

ANNEX I.B – DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred

Authorized representatives of Licensee
Authorized Users
Any individual whose data may be represented within Licensee data when and only to the extent that access to the personal data of these data subjects is required for solving specific support issues related to the Services.

1. Categories of personal data transferred

Authorized representatives of Licensee:
Categories comprise representative properties, e.g., name, phone number, email addresses.
It is Immuta's policy, and Licensee agrees, that representatives of Licensee should only connect to Immuta's platform with a corporate IP address.

Authorized Users:
Categories comprise user ID, debugging ID, date first seen, browser, device type, OS, events such as pageviews, click-ons and actions performed within an Immuta instance such as policy or project creation, purpose or tag management, etc.

It is Immuta's policy, and Licensee agrees, that authorized users of Licensee should only connect to Immuta's platform with a corporate IP address.

Any individual whose data may be represented within Licensee data:
The categories of personal data depend on which personal data the Licensee authorizes Immuta to access in the context of a support request. It is Immuta's policy that authorizing Immuta to access personal data in the context of a support request should be avoided whenever possible and should only be allowed when the rendering of support would be impossible without Immuta's access to such data.

2. 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.

It is not the purpose of the Agreement to transfer sensitive data. Sensitive data shall only be transferred in highly exceptional circumstances except as set forth in Section 2.4 in the DPA. Licensee must take all precautions and shall warrant that Immuta is allowed to have access to such sensitive data.

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

With the exception of transfers that may happen in the context of a specific request for support, all transfers happen on a continuous basis.

4. Nature of the processing

Providing the Services as identified in the Agreement, which essentially entails the automated processing of personal data through Immuta's cloud-based services, and other related internal activities as described below.

5. Purpose(s) of the data transfer and further processing

When Immuta acts as controller:

- account registration;
- account administration;
- billing;
- direct marketing;
- communication with customers;
- license compliance and fraud prevention;
- user experience optimization;

- product and service improvements;
- Other processing operations, as will be performed to comply with applicable laws.

When Immuta acts as processor or sub-processor:
To be able to provide the Services and in particular:

- Providing support to Licensee, including troubleshooting and debugging (preventing, detecting, and repairing problems);
- Activity logging and log and security management;
- Other processing operations, as will be performed to comply with applicable laws.

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

The retention periods for personal data processed by Immuta as controller are aligned to the purposes for which the data is processed and are reviewed annually.

The retention period for personal data processed by Immuta as processor is dependent on the instructions of the Licensee. In any event, Immuta shall stop processing Licensee Data after the end of the provision of the relevant Service within a reasonable period and no later than 90 days after the termination of the Agreement, unless the data has been anonymised.

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

Processing activities include account administration and billing, customer relationship management and direct marketing, hosting, data management and visualization, statistics generation and fraud prevention.

Sub-processing activities include hosting, the management of logs and security, and customer support.

For data processed by Immuta as controller, the personal data will be processed by its processors for as long as necessary for the provision of the service or the pursuance of legitimate internal business purposes, to the extent that the collaboration with the processor has not been terminated before such time. Data retention periods are reviewed annually.

For data processed by Immuta as processor, the duration of the data processing is dependent upon the instructions of Licensee. In any event, Immuta's sub-processors shall stop processing Licensee's personal data after the end of the provision of the relevant Service within a reasonable period and no later than 90 days after the termination of the Agreement, unless the data has been anonymised or unless the collaboration with the sub-processor has been terminated.

ANNEX I.C – COMPETENT SUPERVISORY AUTHORITY

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

The data protection authority competent for the Data Exporter or, if the Data Exporter is not established in the European Union or has not appointed a representative in the European Union, is the data protection authority competent for the data subjects whose personal data are transferred under the clauses.

ANNEX II

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

The technical and organizational security measures taken by Immuta, include the following:

Security Controls at Immuta **Infrastructure Security** Immuta is cloud-native, including all our supporting cloud computing infrastructure and our software solution (Software-as-a-Service). Our cloud computing infrastructure is provided by Amazon Web Services (AWS). This infrastructure is built and managed not only according to security best practices and standards, but also with the unique needs of the cloud in mind. AWS uses redundant and layered controls, continuous validation and testing, and a substantial amount of automation to ensure that the underlying infrastructure is monitored and protected 24x7. Every 24 hours we make a backup which we keep for 7 days. In case of an incident, we can restore this backup immediately.
Physical Security We rely on AWS for the physical security of our supporting cloud computing infrastructure. We also take physical security measures for our own offices (such as badge access and video surveillance).
Product Security We have a clearly software development defined process, ensuring that our software is tested and ready for production use before we deploy our software. We take security measures to protect our software solution from cyber attacks and to detect fraudulent or malicious activities. Our software is monitored and protected by an industry-leading continuous process of cloud security improvement and adaptation which includes active defenses against known and unknown attacks. In addition, we also have periodic security measures carried out by a qualified external party (such as penetration testing). Additional security measures we implement include encrypting your data both at rest and in transit, restricting access based on roles and attributes, applying the need-to-know principle, requiring strong passwords and multi-factor authentication, and monitoring logs.

Data Security In accordance with our DPA, we process personal data in accordance with Data Protection Laws, both in terms of security and data protection. Subprocessors are also required to comply with Data Protection Laws in the agreements we conclude with them. Our software solution is set up in the same region as your infrastructure. Immuta implements strict access control, including purpose-based access control for all categories of personal data. Usage Data is pseudonymised.
Data Retention and Access In accordance with our DPA, we do not retain your personal data longer than necessary. We will retain your personal data for as long as you are an active customer and for a period afterward in accordance with the DPA. In the event your Agreement is terminated or expires, we will delete your personal data 90 days after such an event. In the case of a trial period, we will retain your personal data for 90 days after the trial period ends, unless you request that we delete your data sooner. We only access your personal data on request or with your permission, for example when you sign up for or use our Services or request Support.
Attestation & Certification We can demonstrate that we have appropriate controls in place to mitigate security, availability, confidentiality, processing integrity, or privacy risks. Our security measures are audited annually by an independent and external party in the context of SOC 2 Type 2 attestation and ISO 27001/27701 certification. If you need more information or if you would like to receive a summary of our SOC 2 Type 2 or SOC 3 report, please contact us at security@immuta.com.

ANNEX III
LIST OF SUB-PROCESSORS

The list of (sub-)processors engaged by Immuta is available on Immuta's website [https://www.immuta.com/trust/].

SCHEDULE 2 – ADDITIONAL SCC PROVISIONS

BASED ON EUROPEAN DATA PROTECTION BOARD RECOMMENDATIONS

1. Government Disclosure Requests.

    a. Immuta shall, unless otherwise prohibited by law or a legally binding order of an applicable body or agency, promptly notify Licensee or the applicable data subject of any request for the disclosure of Licensee Personal Data by a governmental or regulatory body or law enforcement authority (including any Supervisory Authority) ("**Disclosure Request**") without responding to such request, unless otherwise required by applicable law (including to provide acknowledgement of receipt of the request). If applicable laws prohibit Immuta from informing Licensee or the applicable data subject of the Disclosure Request, Immuta shall use reasonable efforts to obtain a waiver of such restrictions and shall in any event provide such notification as soon as any relevant restrictions are lifted.

    b. Immuta will review applicable law to evaluate any Disclosure Request, for example the ability of the requesting authority to make the Disclosure Request, and to challenge the Disclosure Request if, after a careful assessment, it concludes that there are grounds under applicable law to do so. When challenging a Disclosure Request, Immuta shall seek interim measures to suspend the effects of the Disclosure Request until an applicable court or other authority has decided on the merits. Immuta shall not disclose Licensee Personal Data requested until required to do so under applicable law. Immuta shall only provide the minimum amount of Licensee Personal Data permissible when responding to the Disclosure Request, based on a reasonable interpretation of the Disclosure Request.

    c. If the Disclosure Request is incompatible with the SCCs or other data transfer mechanism utilized in accordance with Section 4 in this DPA, Immuta will so notify the requesting authority and, if permitted by applicable law, notify the competent EEA government authority with jurisdiction over the Licensee Personal Data subject to the Disclosure Request.

    d. Immuta will maintain a record of Disclosure Requests and its evaluation, response, and handling of the requests. Immuta will provide Licensee with such records relevant to Licensee Personal Data except as prohibited by applicable law or legal process or in the interest in protecting Immuta's legal rights in connection with threatened, pending, or current litigation.

    e. Immuta will maintain internal policies and/or procedures related to the handling of Disclosure Requests.

2. Immuta has, as of the Effective Date, not received any national security orders under Foreign Intelligence Surveillance Act ("FISA") Section 702.

3. As of the Effective Date, no court has found Immuta to be the type of entity defined in 50 U.S.C § 1881(b)(4) eligible to receive process issued under FISA Section 702.

4. Immuta has not purposefully created "back doors" or similar programming in its systems that provide Services that could be used to access the systems and/or Licensee Personal Data, nor has Immuta purposefully created or changed its business processes in a manner that facilitates access to Licensee Personal Data or its systems that provide the Services. To the best of Immuta's knowledge, United States Data Protection Laws do not require Immuta to create or maintain "back doors" or to facilitate access to Licensee Personal Data or systems that provide Services or for Immuta to possess or provide the encryption key in connection with a United States Disclosure Request.

5. The parties shall each monitor Data Protection Laws, and upon any changes to the same, either party may request to amend the DPA in such a manner as it determines necessary to comply with such amended Data Protection Laws and the parties shall thereafter negotiate in good faith an amendment to this DPA. If the parties are unable to agree on an amendment within thirty (30) days, a) either party may terminate the DPA as set forth in the Agreement, b) the parties may explore options to further protect the Licensee Personal Data or alter the Processing so as to mitigate certain risks identified by the parties, or c) request the destruction and/or return of Licensee Personal Data as set forth in the DPA.

6. Immuta shall use reasonable efforts to assist Licensee and its Data Subjects, as instructed by Licensee (in accordance with Section 6 of the DPA), regarding Disclosure Requests, unless prohibited by applicable law, for example to provide information to Licensee in connection with the Data Subject's efforts to exercise its rights and obtain legally available redress, provided Immuta shall not be required to provide Licensee or Data Subjects with legal advice.

7. Immuta will maintain internal policies and/or procedures related to transfers of Personal Data of customers. Immuta has procedures for applicable personnel to receive information, as appropriate, regarding applicable transfers of Licensee Personal Data, where such information may include an explanation of the necessity of the transfer and any data protection safeguards in scope. Personnel responsible for reviewing requests to transfer Personal Data of customers may include IT, security, compliance, and legal personnel.

8. In the event Immuta receives a request to voluntarily disclose unencrypted Licensee Personal Data to a government authority, Immuta will use reasonable efforts to first obtain Licensee's consent, either on its behalf or on behalf of the relevant Data Subject, unless Immuta has already obtained Licensee's implied consent.