Immuta Inc.
Master Subscription Agreement

1. SCOPE OF AGREEMENT AND GRANT OF LICENSE

1.1. Scope of Agreement. Immuta develops, markets and makes available access to certain software programs and individual program modules (collectively, "Software"), as well as related products and services, to its end user customers via either a software-as-a-service methodology or an on-premise deployment (such Software, products and services, collectively, the "Services"). Access to the Services is provided pursuant to this Agreement, and the specific Services and Software are set forth in a subscription form executed by the parties (each, an "Subscription Form"). Access to the Services includes use of any associated documentation, including user manuals, report templates, screen layouts and other materials made available in any form by Immuta to Licensee in connection with the Services (the "Documentation"). Any corrections, updates and/or other software provided to Licensee by Immuta shall be deemed Software or Services under this Agreement.

1.2. Access to Services. Subject to the terms and conditions of this Agreement, Immuta hereby grants to Licensee a limited, non-exclusive and non-transferable right during the applicable Subscription Term (as defined below) to access the Software (in object code form only) via the Services and to use the Services solely for its internal business purposes as set forth in this Agreement. Access to the Software and Documentation is provided as part of the Services, and as such they are licensed, not sold..

1.3. Documentation. Licensee shall be entitled to (a) use the Documentation internally solely to support its authorized use of the Services and (b) make that number of copies of the Documentation as are reasonably required for it to exercise its rights under clause (a). Any such copies shall include all trademarks or other proprietary legends where and as set forth in the original. Licensee agrees not to provide access to the Documentation to any third party except Authorized Users (as defined below).

1.4. Restrictions. Licensee shall not, and shall not attempt to (and shall not authorize or allow Authorized Users or any third party to attempt to): (a) disassemble, reverse engineer, decompile, or otherwise attempt to derive source code from the Software in whole or in part; (b) modify, adapt, create derivative works based upon, or translate the Software; (c) assign, transfer, re-license, sublicense, lease, loan, resell, distribute or otherwise grant any rights in the Software or the Services in any form to any other party, including commercial time-sharing, rental, or service bureau use; or (d) use the Software, the Services or the Documentation on behalf of any third party or for any purpose other than monitoring, collecting, analyzing and using Licensee Data (as defined below) for Licensee's internal business purposes.

1.5. Authorized Users. The Services shall be used solely by employees, independent contractors and third-party service providers of Licensee authorized by Licensee to use the Services under the rights granted pursuant to this Agreement, solely for Licensee's business purposes, and for which all applicable fees have been paid ("Authorized Users"). Licensee shall cause all Authorized Users to comply with Licensee's obligations under this Agreement and shall be responsible for any noncompliance with such obligations by any Authorized User.

1.6. Licensee Responsibilities. Licensee shall: (a) ensure that access credentials to the Services are kept confidential and access is enabled only through encrypted connections; (b) give employees appropriate permission levels to the Services, monitor their activities, and revoke access to the Services within 24 hours of termination of employment; (c) alert Immuta within 72 hours of any security incidents that could impact the Services or Immuta's systems (e.g., compromised credentials, a stolen laptop, and network compromise); (d) maintain the security of servers and other devices (including, but not limited to, by implementing sufficient password protocols and the physical and environmental controls necessary to ensure availability of the Services); (e) maintain up-to-date operating

system patching and active anti-malware on devices used to connect to Licensee's environment; (f) comply with all applicable laws and regulations in its use of the Services and in its collection, disclosure and use of Licensee Data, including those laws and regulations relating to personal data protection and privacy; (g) be solely responsible for configuring the Service's policy engine to act on Licensee Data (as defined below) in a manner that conforms with Licensee's rules, applicable laws and regulations, and reasonable privacy and security standards; and (h) be solely responsible for providing and installing within the Service's web interface ODBC drivers for any third party databases to which the Service will connect.

2. TERM OF AGREEMENT, SUBSCRIPTION TERM AND TERMINATION

2.1. Term of Agreement. The term of this Agreement shall commence upon the Effective Date and continue until expiration or termination of the last Subscription Form.

2.2. Subscription Term. The initial subscription term of the Services shall be as specified in the applicable Subscription Form and shall commence on the date on which the Service is made available to Licensee. Subscriptions shall renew automatically for additional terms equal in duration to the expiring subscription term, unless either party gives the other party written notice of its intent not to renew the term at least thirty (30) days prior to the expiration of the then-current term (the initial subscription term and each renewal subscription period, collectively, the "Subscription Term").

2.3. Termination. Either party may, at its option and without further notice, immediately terminate this Agreement and the licenses granted hereunder if the other party: (a) breaches any material obligation under this Agreement and such breach is not cured within thirty (30) days after the receipt of written notice of the alleged breach; (b) admits in writing its inability to pay its debts generally as they become due; (c) makes a general assignment for the benefit of creditors; (d) institutes proceedings to be adjudicated a voluntary bankrupt, or consents to the filing of a petition of bankruptcy against it; (e) is adjudicated by a court of competent jurisdiction as being bankrupt or insolvent; (f) seeks reorganization under any bankruptcy act, or consents to the filing of a petition seeking such reorganization; or (g) ceases to do business as itself or through a successor.

2.4. Effect of Termination. Upon the effective date of termination of this Agreement, all licenses granted hereunder shall terminate, and Licensee shall immediately cease any and all use of the Services and deinstall all instances of Software installed in Licensee's environment. Within ninety (90) days of termination, Immuta will destroy all instances of Licensee Data (as defined in Section 4.1). The terms of Sections 2-5, 8 and 10-12 shall survive termination or expiration of this Agreement.

3. SERVICES FEES AND PAYMENT TERMS

3.1 The Services Fees are listed on the Subscription Form. Services fees shall be due and payable annually in advance unless otherwise stated on the Subscription Form, net thirty (30) days after the invoice date. Immuta will invoice Licensee upon commencement of the Subscription Term. All fees and charges hereunder are exclusive of all federal, state, municipal, and other governmental excise, sales, use, customs, value-added, and other taxes and import fees or duties now in force or enacted in the future. Licensee agrees to pay on or before their due date all such taxes, fees, duties and charges which arise out of or in connection with this Agreement or any license granted herein, but excluding taxes based on Immuta's net income. In the event Licensee purchases the Services from an authorized reseller of Immuta, then pricing, payment, delivery, and related terms will be agreed between Licensee and the reseller.

3.2 In the event of any overdue payments, Immuta reserves the right to charge interest from the due date at the lesser of the rate of one percent (1%) per month (or the maximum rate permitted by law) and/or to suspend Licensee's access to the Services. All costs of collection, including reasonable attorneys' fees, shall be paid by Licensee. Unless otherwise specifically provided in this Agreement, all Services fees are non-refundable.

3.3 Immuta reserves the right to increase the applicable subscription fee for each renewal term by no more than the greater of six (6%) percent or the annual increase in the Consumer Price Index, provided notice of any such increase is provided to Licensee no later than sixty (60) days prior to the expiration of the then-current Subscription Term. In the event that Licensee increases the number of units used by Licensee during the Subscription Term, Immuta may invoice Licensee for an amount equal to the annual Subscription Fee per unit

multiplied by the increased number of units (prorated, as necessary).

4. LICENSEE DATA

4.1 As between Licensee and Immuta, Licensee has and shall retain sole and exclusive title and ownership of all Licensee Data and all intellectual property rights therein. "Licensee Data" means any data and information that are (a) provided, submitted and/or otherwise inputted by Authorized Users into the Services in the course of utilizing the Services, (b) subject to Immuta's intellectual property rights in the Services, generated by Licensee or any Authorized User in the course of utilizing the Services, or (c) otherwise collected by Immuta from Licensee or any Authorized User; provided, however, that Licensee Data does not include Usage Data (as defined below) or data, information or materials lawfully obtained by Immuta from third parties.

4.2 Notwithstanding the foregoing, Immuta shall have the right to use and disclose Licensee Data to: (a) provide the Services under this Agreement; (b) monitor Licensee's use of the Services for security and other internal business purposes; (c) enforce the terms of this Agreement; and (d) generate Usage Data for statistical and other analysis, including to improve the Services. "Usage Data" means information and data relating to the manner in which Licensee is using the Service.

4.3 Immuta handles and protects Licensee Data in accordance with this Agreement and Immuta's privacy policy, which is available at https://www.immuta.com/legal/privacy-policy/.

5. INTELLECTUAL PROPERTY RIGHTS

Immuta and its licensors are the sole owners of the Services, Software, Documentation and Usage Data (including any modifications or improvements made thereto) and of all copyright, trade secret, patent, trademark and other intellectual property rights therein and thereto throughout the world. Neither this Agreement nor any Subscription Form provide Licensee or any Authorized User with title to or ownership of the Services, Software, Documentation or Usage Data, or to any copies or modifications thereof, but only the limited license granted under the terms and conditions of this Agreement.

6. SECURITY POLICY; BUSINESS CONTINUITY PLAN

Immuta maintains administrative, physical and technical controls, processes, and procedures, consistent with applicable industry standards, which are designed the protect the security and confidentiality of the Service and Licensee Data ("Security Controls"). Security Controls include, but are not limited to:

- Formalized policies and procedures for all internal control requirements
- System logging and monitoring
- Patch and change management
- Vulnerability management
- Antivirus/antimalware software
- Identity and access (logical and physical) management
- Multi-factor authentication
- Secured remote access
- Firewall and network security group management
- Backup management and Business continuity
- Incident management

Security Controls have been independently audited and certified against the AICPA SOC2 Type2 standard. A copy of Immuta's SOC2 Type2 report is available on request and will be considered the Confidential Information of Immuta.

7. SUPPORT SERVICES

Immuta provides standard support Services (the "Support Services") as described in the then-current Immuta Support Policy available at: https://www.immuta.com/legal/ (the "Support Policy").

8. CONFIDENTIAL INFORMATION

8.1 Each party agrees that any non-public information, data, materials or know-how, including without limitation, prices, fees, methods, software, algorithms, documentation, drawings, processes, techniques, technical and other business information which may be supplied by one party to the other party in connection with this Agreement, whether orally or in writing, that are either designated as proprietary and/or confidential at the time of disclosure, or which, by its nature, would be considered by a reasonable person to be proprietary and/or confidential (collectively, "Confidential Information"), are confidential and constitute valuable assets of the disclosing party. Without limiting the foregoing, (a) Immuta acknowledges and agrees that Licensee Data are Confidential Information of Licensee, and (b) Licensee acknowledges and agrees that the Services, Software, Documentation, Usage Data, and statistical performance results of any evaluation or benchmark tests run on the Services by or on behalf of either Licensee or Immuta are Confidential Information of Immuta.

8.2 Confidential Information does not include: (a) information which is or becomes publicly available other than through disclosure in breach of this Agreement; (b) information disclosed or made available by a third party without restriction and without breach of an obligation of confidentiality; (c) information independently developed by one party without use of or reference to any Confidential Information of the other party, as evidenced by applicable documentation; or (d) information which was already known by the receiving party at the time of disclosure.

8.3 During the term of this Agreement and for five (5) years thereafter, each party agrees to use the Confidential Information only for the purposes specifically authorized in this Agreement, to hold such Confidential Information in strict confidence, and not to disclose any of the Confidential Information to any third party except as necessary to provide the Services or as otherwise contemplated under this Agreement. Each party agrees to limit access to Confidential Information to those employees and contractors whose use of or access thereto is necessary for the authorized use of the Confidential Information under this Agreement. Licensee agrees not to use, or allow any third party to use, any Confidential Information to aid in the development or marketing of any product similar to or competitive with the Services.

8.4 The obligations of non-disclosure set forth above shall not apply to the extent that a party is legally required to produce Confidential Information pursuant to a subpoena or other legal process or order of a court of competent jurisdiction, provided that such party provides prompt written notice to the other party of such process or order and produces only that portion of the applicable Confidential Information legally required under such process or order after the other party has had an opportunity to challenge such process or order.

8.5 Upon written request from the disclosing party, the receiving party shall return to the disclosing party all Confidential Information in the receiving party's possession or control, and all copies thereof, or, at the disclosing party's option, certify its permanent, secure destruction in writing.

9. Personal Data Protection

9.1. Compliance with data protection law. As part of providing the Services, personal data of Authorized Users and of others in the sense of Article 4 of EU Regulation 2016/679 or the General Data Protection Regulation ("GDPR") may be processed. Both Immuta and Licensee acknowledge that such processing may take place and agree to comply with their respective obligations under the GDPR and applicable national data protection legislation (together referred to as "Data Protection Law").

9.2. Immuta's and Licensee's role. When Immuta processes personal data of Licensee's authorized representatives when Licensee purchases, renews or cancels its subscription or when Immuta processes Usage Data,

Immuta acts as a controller. For all other personal data processed by Immuta in the context of providing the Services, Immuta acts as a processor:

- when Licensee uses the Services to process personal data for Licensee's own purposes, Immuta acts as a processor and Licensee acts as a controller;
- when Licensee uses the Services to provide itself services to a customer, and Licensee therefore processes personal data as a processor on behalf of said customer, Immuta processes personal data when providing the Services as a sub-processor.

9.3. Immuta as controller. When Immuta processes personal data in the context of the Agreement as a controller, Immuta will provide, to the extent required under Data Protection Law, the individuals concerned with a privacy statement before any processing takes place. By entering into this Agreement, Licensee understands and accepts that personal data will be transferred to the United States of America for account registration, administration, billing, communication with customers, direct marketing, fraud prevention, user experience optimization and product and service improvements. Such transfer shall be governed by the Standard Contractual Clauses (applying Module One) set forth in Exhibit B of this Agreement. The Standard Contractual Clauses govern the collection and all further processing of personal data by Immuta as a controller for and under this Agreement. In case of a conflict between the Standard Contractual Clauses and the provision of the Agreement, the Standard Contractual Clauses shall prevail.

9.4. Immuta as processor. When Immuta processes personal data on behalf of Licensee as a processor or a sub-processor, Immuta will process the personal data of Authorized Users, and may process the personal data of other individuals represented within Licensee Data when and only to the extent that it is necessary for specific support issues. This processing, including data transfers outside the EEA, will be performed only (a) upon Licensee's documented instructions and at a minimum for the purpose of complying with the obligations of Immuta under the Agreement and (b) to allow Immuta to comply with its legal or judicial obligations. If it is for the purpose of performing Immuta's legal or judicial obligations, Immuta will inform Licensee immediately in writing in advance thereof, unless Immuta is legally or judicially not allowed to do so. By entering into this Agreement, Licensee instructs Immuta to transfer personal data processed as part of the Services to the United States of America.

Such transfer by Immuta shall be governed by the Standard Contractual Clauses (applying Module Two when Licensee acts as controller or applying Module Three when Licensee acts as processor) set forth in Exhibit B of this Agreement. The Standard Contractual Clauses govern the collection and all further processing of personal data by Immuta as a processor for and under this Agreement. In case of a conflict between the Standard Contractual Clauses and the provision of the Agreement, the Standard Contractual Clauses shall prevail. Immuta will take all measures required pursuant to Article 32 GDPR. These security measures are outlined in Annex II of the Standard Contractual Clauses. These measures may be updated from time to time to allow Immuta to take the evolving threat landscape into account.

Immuta's list of sub-processors in the sense of Article 9 of the Standard Contractual Clauses is available on its website [https://www.immuta.com/trust/]. When Immuta, acting itself as a processor or sub-processor, engages new sub-processors in the sense of Article 9 of the Standard Contractual Clauses, Licensee shall have ten (10) days to object to the addition or replacement of a sub-processor after the publication of such addition or replacement on the aforementioned list. If the Licensee does not object within this ten-day period, the addition or replacement shall be deemed accepted. Any objection must include a detailed explanation of the reasons for the objection, must be based solely on reasonable grounds related to data protection concerns and must be sent in writing to Immuta. In case of a reasonable and valid objection, Parties shall negotiate in good faith to find a resolution. In the event Parties are not able to find a resolution to a reasonable and valid objection, Licensee, as its sole and exclusive remedy, may provide written notice to Immuta terminating the Agreement with respect only to those aspects of the Services which cannot be provided by Immuta without the use of the new sub-processor.

10. LIMITED WARRANTY AND DISCLAIMERS

10.1. Limited Warranty. Immuta warrants that, during the Subscription Term, the Services will substantially conform to the specifications contained in the Documentation. Immuta's sole responsibility under this limited warranty shall be to use commercially reasonable efforts to correct or replace the portion of the Services which fail to conform

to such limited warranty, provided, however, that Licensee has reported in writing to Immuta any defect or error claimed to be a breach of such warranty. Immuta shall have no liability under the foregoing limited warranty if: (a) Licensee, an Authorized User or any third party acting on Licensee's behalf modifies the Services; (b) Licensee fails to give Immuta written notice of the claimed breach of warranty in a timely manner; (c) the failure to conform is caused in whole or part by persons other than Immuta, or by products, equipment, software, services or operating environments not furnished by Immuta; or (iv) Licensee fails to implement any correction, update, enhancement, improvement, expansion or revision thereto which Immuta has provided to Licensee. Licensee shall be exclusively responsible for the supervision, management and control of Licensee's and each Authorized User's use of the Services and for the application and configuration of the Services to Licensee's business.

10.2. Disclaimer. EXCEPT AS OTHERWISE EXPRESSLY AGREED IN WRITING, THE EXPRESS WARRANTIES SET FORTH IN SECTION 9.1 ARE THE ONLY WARRANTIES GIVEN BY IMMUTA WITH RESPECT TO THE SERVICES, SOFTWARE, AND DOCUMENTATION, WHICH ARE OTHERWISE PROVIDED ON AN AS-IS, AS-AVAILABLE BASIS. IMMUTA AND ITS LICENSORS DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, BY OPERATION OF LAW OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, IRRESPECTIVE OF ANY PREVIOUS COURSE OF DEALING BETWEEN THE PARTIES OR CUSTOM OR USAGE OF TRADE. IMMUTA DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE.

11. LIMITATION OF LIABILITY

EXCEPT WITH RESPECT TO THE PARTIES' INDEMNIFICATION OBLIGATIONS, CONFIDENTIALITY VIOLATIONS, LICENSEE'S OBLIGATION TO PAY ANY AMOUNTS OWED HEREUNDER, OR A PARTY'S LIABILITY FOR INFRINGEMENT OR MISAPPROPRIATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY, IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY UNDER THIS AGREEMENT DURING ANY CONTRACT YEAR EXCEED THE FEES PAID TO IMMUTA BY LICENSEE DURING SUCH CONTRACT YEAR. IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY LOST OR ANTICIPATED REVENUE OR PROFITS OR EXPECTED SAVINGS, LOST OPPORTUNITIES, DIMINUTION OF VALUE OR LOSS OF GOODWILL, OR FOR ANY INCIDENTAL, PUNITIVE, EXEMPLARY, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, SUCH AS CLAIMS OF THIRD PARTIES, REGARDLESS OF WHETHER IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

12. INDEMNIFICATION

12.1 Immuta shall defend Licensee against any claim or action brought against Licensee, and will indemnify and hold harmless Licensee from and against any damages, liabilities, costs or expenses (including reasonable attorneys' fees) awarded by a final judgement of a court or included as part of a final settlement, to the extent based upon the infringement by the Services of any United States patent, trademark or copyright of a third party ("Claims"), provided that (a) Immuta is promptly notified in writing of any Claim, (b) Immuta has sole control over the defense and/or settlement of the Claim, and (c) Licensee gives Immuta all available information and assistance (at Immuta's expense) to enable Immuta to do so.

12.2 In addition, if, as the result of any Claim, Licensee is enjoined from using the Services, Immuta, at its sole option and expense, may: (a) procure the right for Licensee to continue to use the Services; (b) replace or modify the Services so as to make them non-infringing (without materially impacting functionality or performance); or (c) if Immuta is not able to accomplish either of the foregoing alternatives on commercially reasonable terms, terminate Licensee's license to the Services and refund to Licensee that portion of the fee prepaid for the then-current Subscription Term which reflects the unused portion of such Subscription Term.

12.3 The foregoing indemnity shall not apply if the Claim results from: (a) Services that have been modified by anyone other than Immuta or its subcontractors; (b) Licensee's use of the Services with software, hardware, data or services not provided by Immuta; (c) misuse of the Services or other breach of this Agreement; (d) use of other than the most current, unaltered corrections and updates to the Services which have been provided to Licensee at no additional charge; or (e) compliance by Immuta with designs, plans or specifications furnished by or on Licensee's behalf. Immuta shall not be liable hereunder for any settlement made by Licensee without Immuta's advance written

approval. Licensee will indemnify, defend and hold harmless Immuta from and against any Claims brought against Immuta arising out the circumstances described in this paragraph.

12.4 THE FOREGOING STATES THE ENTIRE LIABILITY OF IMMUTA WITH RESPECT TO ANY THIRD PARTY INFRINGEMENT CLAIMS.

13. GENERAL

13.1. Marketing Usage. Immuta may use Licensee's name and logo in its marketing materials and on its website. Immuta also may have Licensee serve as a reference to showcase how they use Immuta.

13.2. Commercial Computer Software. If any Services or Documentation are acquired by or on behalf of an agency or instrumentality of the United States government, Licensee acknowledges and agrees that such Services or Documentation are "commercial computer software" or "commercial computer software documentation" developed at private expense and that, absent a written agreement to the contrary, the government's rights with respect to such Services or Documentation shall be as set forth in this Agreement, pursuant to FAR § 12.212(a) and/or DFARS § 227.7202-1(a), as amended and as applicable.

13.3. Force Majeure. Notwithstanding anything in this Agreement to the contrary, no default, delay or failure to perform on the part of either party, excluding Licensee's payment obligations, shall be considered a breach of this Agreement if such default, delay or failure to perform is due to causes beyond such party's reasonable control, including, but not limited to, strikes, lockouts or other labor disputes, riots, civil disturbances, actions or inaction of governmental authorities or suppliers, epidemics, war, embargoes, severe weather, fire, earthquakes, acts of God or the public enemy, nuclear disasters, the infrastructure of the Internet, or default of a common carrier.

13.4. Choice of Law. This Agreement and all claims related to it shall be construed and governed in all respects according to the laws of the State of Delaware, without regard to any conflict of law provisions. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

13.5. Export Laws. Neither party shall commit any act or request the other party to commit any act which would violate the export control laws, rules or regulations of the United States or any other country.

13.6. Waiver. No waiver or failure to exercise any option, right or privilege under the terms of this Agreement by either of the parties hereto on any occasion or occasions shall be construed to be a waiver of the same on any other occasion or of any other option, right or privilege.

13.7. Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, such provision shall be changed and interpreted so as to best accomplish the objectives of the original provision to the fullest extent allowed by law and the remaining provisions of this Agreement shall remain in full force and effect.

13.8. Assignment. Neither party may assign this Agreement without the other party's prior written consent, except (a) to an affiliate, (b) in the event of a merger or the sale of all or substantially all of such party's assets or stock, or (c) in the case of an assignment by Immuta of monies due or becoming due. In any such event, any assignee shall comply with all of the terms and conditions of this Agreement.

13.9. Independent Contractors. The parties are independent contractors, and this Agreement will not establish any relationship of partnership, joint venture, employment, franchise, or agency between the parties.

13.10. Trial Deployments. In the event Licensee conducts a proof-of-concept, trial or other test of the Service, Licensee agrees that its use of the Service will be limited to evaluation purposes only (and not for any commercial or production use) for the agreed upon period. In such cases, the Service is provided as-is, with all faults,

with no warranties or representations (express or implied) whatsoever, and the service levels in Exhibit A shall not apply. Immuta shall have no liability whatsoever in connection with such activities.

13.11. Entire Agreement. This Agreement and any Exhibits hereto, together with the Support Policy and any Subscription Forms, contain the entire understanding and agreement between Licensee and Immuta and supersede all prior agreements or understandings, oral or written, relating to the subject matter hereof. Except as otherwise provided herein, no modification, amendment, or waiver of any provision of this Agreement will be effective unless in writing and signed by the party against whom the modification, amendment or waiver is to be asserted. The parties agree that any preprinted or standard terms or conditions in any invoice or purchase order shall be of no effect. In the event of any conflict or inconsistency between an Subscription Form and this Agreement, the Subscription Form shall control.

13.12. Future Commitments. Immuta has made no commitments or promises orally or in writing with respect to delivery of any future software features or functions. In relation to any future software features or functions, all presentations, RFP responses and/or product roadmap documents, information or discussions, either prior to or following the date herein, are for informational purposes only, and Immuta has no obligation to provide any future releases or upgrades or any features, enhancements or functions, unless delivered under a support program or specifically agreed to in writing by both parties. Customer acknowledges that no purchasing decisions are based upon any future software features or functions.

EXHIBIT A
SERVICE LEVELS

The following applies to Services provided by Immuta as software-as-a-service solution in a production environment:

1. Service Availability. Immuta will use commercially reasonable efforts to provide 99.9% Service Availability. Service Availability will be calculated on a monthly basis using the following formula: Actual Availability divided by Expected Availability (expressed as a percentage).

2. Definitions. The following definitions will apply with respect to the calculation of Service Availability:

(a) "**Actual Availability**" means (in minutes) Expected Availability minus Unpermitted Downtime.

(b) "**Expected Availability**" means (in minutes) seven (7) days per week, twenty-four (24) hours per day.

(c) "**Downtime**" means the time (in minutes) that users of the Services are not able to access the Services due to failure, malfunction or delay.

(d) **"Permitted Downtime"** includes Downtime relating to (i) Maintenance, (ii) the facilities, infrastructure, network, products or services of Licensee (or any supplier, subcontractor or representative of Licensee), (iii) the acts, omissions, products or services of a third party, (iv) the negligence, willful misconduct or breach of this Agreement by Licensee, or (v) any other cause not within Immuta's reasonable control.

(e) **"Unpermitted Downtime"** means Downtime minus Permitted Downtime.

(f) "**Maintenance**" means time (in minutes) that the Services are not accessible to Licensee due to maintenance of the Services, including maintenance and upgrading of the Software and hardware used by Immuta to provide the Services. Maintenance includes scheduled maintenance and unscheduled or emergency maintenance. For any maintenance expected to cause more than momentary Downtime, Immuta will use commercially reasonable efforts to provide Licensee with at least two business days' prior notice of any scheduled maintenance or sixty minutes' advance written notice for unscheduled, emergency maintenance. Immuta will provide such notice to Licensee by email to an address provided by Licensee. Maintenance in any given month will not exceed eight (8) hours per month. Any time during which the Services are unavailable to Licensee due to maintenance or other activity by Immuta for which Immuta fails to give notice, which exceeds the permitted time allotment, or which occurs outside of the foregoing permitted hours will be included in the calculation of Downtime. For any maintenance expected to cause more than momentary Downtime, Immuta will use commercially reasonable efforts to schedule all scheduled maintenance windows beginning at 8:00 p.m. Eastern Time or starting between 8:00 p.m. Eastern Time Friday and concluding prior to end of day Sunday Eastern Time.

EXHIBIT B
STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

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

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

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

Intentionally left blank

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

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

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

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

8.2 Transparency

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

(iv) of its identity and contact details;

(v) of the categories of personal data processed;

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

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

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

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

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

8.3 Accuracy and data minimisation

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

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

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

8.4 Storage limitation

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

8.5 Security of processing

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

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

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

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

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

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

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

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or

agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

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

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

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

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

8.9 Documentation and compliance

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

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

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 rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller 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, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. 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 or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) 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 30 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. 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.

MODULE THREE: Transfer processor to processor

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

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

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

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

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

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

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

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

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

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

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

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

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

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

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

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

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

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

MODULE TWO: Transfer controller to processor

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

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

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

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 12

Liability

MODULE ONE: Transfer controller to controller

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

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

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

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

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient;

the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

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

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

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

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

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

(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 [for Module Three: , if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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.

[For Module Three: The data exporter shall forward the notification to the controller.]

(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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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 [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

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

Clause 17

Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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 the Netherlands.

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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 the Netherlands.

(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

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: 7878 Diamondback Drive, Suite C, College Park, MD 20740, 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

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.

2. Categories of personal data transferred

Authorized representatives of Licensee:
Categories comprise representative properties, e.g., name, phone number, email addresses.

Authorized Users:
Categories comprise user properties, e.g., account name, user ID, user name, email addresses, IP addresses, session properties, e.g., time, platform, country, session ID, and events, e.g., pageview, click-ons and other event properties.

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.

3. 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 when such is required for the rendering of support as requested by Licensee. Licensee

must take all precautions and shall warrant that Immuta is allowed to have access to such sensitive data for the sole purpose of responding to Licensee's request for support.

4. 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. Immuta implements strict access control, including purpose-based access control for all categories of personal data.

5. 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.

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

When Immuta acts as controller:

- account registration;
- account administration;
- billing;
- direct marketing;
- communication with customers;
- 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.

7. 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.

8. 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, 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 before the end of the 90-day period.

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 defined process for creating high quality software, ensuring that our software is well tested and ready for production use before we roll out 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).

We also take many other security measures to ensure that your data is safe (such as 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, monitoring logs, etc.).
Data Security We always process your data in accordance with the applicable legislation, both in terms of security and data protection. Every other party we work with also complies with the applicable legislation through the agreements we conclude with them. We do not keep your data longer than necessary. We will hold your data for as long as you request our services. In case of termination, we will delete your data 90 days after the termination. In the case of a trial period, we will retain your data for 90 days after the trial period ends, unless you request that we delete your data sooner. Our software solution is set up in the same region as your infrastructure. We only access your data on request or with your permission.
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. If you need more information or if you would like to receive a copy of our SOC2 or SOC3 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/].