SAAS SOLUTION CUSTOMER AGREEMENT

Last updated August 14, 2024

This SaaS Solution Customer Agreement (this "**Customer Agreement**") is entered into by and between Zoloz Pte. Ltd. ("**Company**") and the legal entity that intends to use the Solution and agrees to these terms herein ("**Customer**"), each a "**Party**", and collectively the "**Parties**". The reference to this Customer Agreement consists of the terms and conditions (including those of any schedules or addendums attached, referenced or incorporated herein, including to the extent applicable Order Forms, Solution Specific Terms, Data Processing Agreement("**DPA**"), and/or Customer Terms (if Customer procures Solution from a Reseller)) governing Customer's downloading of, installation of, access to and use of the Solution (as defined below) through a "software as a service" ("**SaaS**") arrangement.

BY (1) CLICKING AN "ACCEPT" (OR SIMILAR) BUTTON, (2) EXECUTING AN ORDER FORM ONLINE OR OFFLINE, OR (3) ACCESSING OR USING ANY SOLUTION, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS CUSTOMER AGREEMENT. AN INDIVIDUAL WHO IS ACCEPTING ON BEHALF OF A LEGAL ENTITY REPRESENTS THAT HE/SHE HAS THE AUTHORITY TO BIND SUCH ENTITY (AND ITS RELEVANT AFFILIATES, AS APPLICABLE) TO THIS CUSTOMER AGREEMENT.

1. Definitions

1.1. Unless the context otherwise requires, capitalised terms used in this Customer Agreement shall have the meaning specified in **Schedule 1**.

2. Provision of Solutions

2.1. In consideration for Customer's payment of the Charges, and subject to the terms and conditions set forth in this Customer Agreement, the applicable Order Forms, Solution Specific Terms and/or Customer Terms (if applicable), Company grants Customer the right to access and use the Solution during the Term and within the Territory specified, on a non-exclusive, revocable, non-transferable, non-sublicensable basis, solely for the purpose of Customer providing the Customer Services to its End Users.

2.2. To access and use Solution, Customer must have a user account associated with a valid email address and a valid form of payment. Customer shall be responsible for the information it provides to create the account, the security of its log-in credentials for the account, and all activities that occur under its account (regardless of whether such activities are undertaken or authorized by Customer). Customer must promptly notify Company about any possible misuse of Customer's account or authentication credentials or any Security Incident related to Solution.

2.3. Company shall have the right to Process any Customer Data that it has access to (including transfer of any such Customer Data to third parties for Processing) for the provision, development and maintenance of Solution under this Customer Agreement and in accordance with the Data Processing Agreement (to the extent any Personal Data is Processed by Company).

3. Modifications

3.1. Modifications to Solution. Company may release Updates to Solution from time to time, which may add, suspend, substitute, replace, remove or discontinue any component, feature or function of Solution without any liability towards Customer and/or any End Users. Such Updates shall form part of Solution and be subject to this Customer Agreement (including any additional Solution Specific Terms, if applicable).

3.2. Modifications to Agreement. Company reserves the right to alter, modify, add to or otherwise vary this Customer Agreement at any time. Company will notify Customer of such changes by commercially reasonable means, including by sending emails to Customer or posting revised Customer Agreement on the applicable webpage. Customer shall be bound by this Customer Agreement so amended, and such other terms as may be incorporated by reference, if Customer continues to download, install, access and/or use Solution after such notice.

4. <u>Customer Requirements</u>

4.1. Customers must:

(a) comply with all Relevant Laws (including all Relevant Privacy Laws), Documentation, security procedures, technical standards, system and data security requirements, directions, policies and rules, as notified by Company from time to time;

(b) take appropriate security, protection and back-up action in accordance with the requirements specified in the Documentation and are otherwise suitable for the purposes of accessing Solution (including preventing a Security Incident, and applying any appropriate encryption over any Transferred Personal Data) and providing Customer Services. At Company's request, provide Company with information about its security procedures and other measures in Customer Systems that are sufficient to demonstrate to Company the adequacy of those procedures and measures;

(c) use commercially reasonable efforts to prevent and terminate unauthorized access to and use of Solution or Customer Services, as applicable; and shall prevent a Security Incident or unauthorised or unlawful use, destruction, alteration or loss of data, information or software contained therein;

(d) only use an API or SDK specified and permitted by Company to access and use Solution; and ensure that it does not make any API calls that would affect or otherwise create a deficiency in the operation of Solution;

(e) in a timely manner, cooperate with Company, Reseller (if applicable) and/or any person designated by Company, and provide information, data, equipment, systems, materials and data interfaces and all other resources as reasonably necessary for Company to properly deliver Solution and perform its obligations under this Customer Agreement or Reseller Agreement (if applicable);

(f) obtain all relevant Regulatory Approvals and all third party consents (including Relevant Data Consents), and determine any restrictions applicable to its use of Solution or provision of Customer Services under the Relevant Laws;

(g) promptly notify Reseller (if applicable) and Company in writing if it becomes aware of any complaint or investigation under, or relating to, any Relevant Privacy Laws or Relevant Data Consents, to the extent permitted by such Relevant Laws, or any circumstances that may lead to any such complaint or investigation; and act promptly in the resolution of any such complaint, investigation or circumstances;

(h) take all such steps as Reseller (if applicable) or Company reasonably requires to facilitate Reseller's and Company's compliance with any of the Relevant Privacy Laws or Relevant Data Consents that apply to the Customer Services;

(i) promptly notify Reseller (if applicable) and Company in writing if it becomes aware of any changes to a Relevant Privacy Law that may cause the Customer Services, Customer's business, or the Processing of Data by, operations of, or conduct of, Customer relating to the Customer Terms (if applicable), to breach such Relevant Privacy Law;

(j) back up Data in accordance with good information technology practices, Relevant Laws and Relevant Data Consents;

(k) procure that any of its Affiliates, its Authorised Personnel and End Users comply with all Relevant Laws, and be responsible for the acts and omissions of all its Authorised Personnel, Affiliates or End Users as if they were the acts and omissions of Customer;

(l) ensure that it implements reasonable security measures (including but not limited to adequate technical and procedural access controls and system security requirements and devices, necessary for data privacy, confidentiality, integrity, authorisation, back-up and virus detection and eradication) to ensure that no unauthorised person may access or use Solution;

(m) conduct screening checks on its Affiliates, Authorised Personnel and/or End Users (as the case may be), to ensure that they are not designated as a Sanctioned Person or located, incorporated or ordinarily resident in any country that is the subject of sanctions, or that they intend to or are likely to use Solution for any Prohibited Activities; and

(n) ensure that neither itself, nor any of its Affiliates, its Authorised Personnel and End Users is a Military End User pursuant to EAR § 744.17 (or the equivalent laws of other countries and jurisdictions in the Territory).

5. Customer Restrictions

5.1. Customer must not, unless expressly permitted by Company or Reseller (if applicable) in writing:

(a) incorporate or grant any other person the right to incorporate Solution into another product to form a new product;

(b) lease, loan, resell, transfer, sublicense or otherwise make available Solution or Documentation, other than to its Affiliates, Authorised Personnel and End Users as permitted in writing;

(c) modify, port, translate, adapt, alter, frame or create derivative works based on Solution or Documentation;

(d) make or attempt to copy (except for installation and backup of Solution as permitted in writing and according to the applicable Documentation), modify, translate, disassemble, decompile, recreate, reverse engineer Solution or any source code, object code, software programs, processes, algorithms, methods, techniques, data, or information embodied in Solution, the relevant portal or platform, or the Documentation, or any part, feature, function, API, SDK or user interface thereof, or extract ideas, algorithms, procedures, workflows or hierarchies from Solution, the relevant portal or platform, or the Documentation or otherwise use Solution for the purpose of creating any other product or service;

(e) change or remove any IP Rights and authorship notices from Solution or Documentation;

(f) access or use or attempt to access or use Solution in any way that causes, or may cause, damage to Solution or other Company Systems or impairment of the availability or accessibility of Solution or other Company Systems;

(g) breach, tamper with, compromise or circumvent any security measures included in Company System, and data security requirements, policies and/or rules notified by Company from time to time;

(h) share, distribute or publish log-in credentials assigned to it except as permitted by Reseller and/or Company (as the case may be);

(i) knowingly do or permit anything to be done which could infringe, invalidate, cancel, harm, challenge, deny, question or contest Company IP;

(j) allow any Company IP to become the subject matter of any charge, lien or encumbrance;

(k) publish or disclose any results of benchmark tests run on any Solution;

(l) disclose, provide or otherwise make available trade secrets in connection with Company IP in any form to any third party;

(m) use Solution to transmit any content, data or information that is unlawful, defamatory, obscene, invasive of another’s privacy or otherwise objectionable;

(n) permit access to or use of Solution, in violation of any Relevant Laws; or

(o) permit access to or use of Solution to exploit for Military End Use or to be resold or transferred to any Military End User.

5.2. Customer acknowledges and agrees that Company may implement and maintain appropriate technology or software technical, organizational, and physical measures including data loss prevention software, to monitor, analyse and facilitate Customer's usage of and access to Solution, as well as to ensure information security of Customer's Systems.

6. End Users

6.1. Customer shall be responsible for the acts and omissions of End Users in access to and use of Solution, and for their compliance with Customer's obligations under this Customer Agreement. If Customer becomes aware of any violation of its obligations under this Customer Agreement caused by an End User, Customer shall immediately suspend or terminate access by such End User and immediately notify Company with necessary details. Company will not provide any support or services to End Users unless otherwise agreed by Company in writing.

7. IP Rights and Data Rights

7.1. IP ownership.

(a) Customer acknowledges and agrees that (i) any and all Company IP is and shall remain owned by Company and/or its licensors (as applicable), (ii) Company owns and shall retain, or licenses and shall retain its rights under licenses for, all Company IP, and (iii) Solution contains, embodies and is based on patented or patentable inventions, trade secrets, copyrights and other IP Rights owned by Company and/or its licensors (as applicable).

(b) Customer's rights with respect to Solution are limited to those granted pursuant to the terms and conditions in this Customer Agreement. All rights in Company IP not expressly granted to Customer under the Customer Terms (if applicable) and this Customer Agreement are reserved by Company. Nothing in the Customer Terms (if applicable) or this Customer Agreement transfers from Company any proprietary right or interest in any Company IP.

7.2. IP infringement. Customer must: (i) promptly notify Company and Reseller (if applicable) in writing of any actual, attempted, threatened or suspected infringement of any of Company IP; and (ii) at the request and expense of Company, provide all reasonable assistance as Company may require in conducting enforcement proceedings or defending proceedings in respect of Company IP.

7.3. Customer Data. Customer authorizes Company during the Term, on a non-exclusive, worldwide, royalty-free basis, to Process any Customer Data that it has access to (including transfer of any such Customer Data to third parties for Processing) for the purpose of facilitating Company to provide Solution. Customer shall have the sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness and IP Rights to use all Customer Data. Company reserves the right to withhold, remove and/or discard Customer Data without notice for any breach by Customer of this Customer Agreement including, without limitation, non-payment.

7.4. Derived Data. Company shall be the sole and exclusive owner of all rights, title and interest (including associated IP Rights) in and to any Derived Data that Company has generated, collected, developed and/or compiled based on any Data or information it has become aware of, directly or indirectly with respect to or in connection with Customer in its provision of Solution.

7.5. Other restrictions. Customer shall not, directly or indirectly: (i) make any copies of any Company IP, or any part thereof, for any purpose other than expressly permitted under this Customer Agreement or otherwise agreed in writing between the Parties; (ii) modify, port, translate, adapt, alter, frame or create derivative works based on Solution; (iii) use Solution for the benefit of any third parties or in any way other than what is expressly permitted in this Customer Agreement; (iv) create internet links to Solution, or frame or mirror the web page(s) from which Solution is accessed; (v) remove, alter or obscure any proprietary notice, labels or marks on any web pages(s) or platforms from which Solution is accessed; or (vi) disable or circumvent any access control or related process or procedure established with respect to Solution.

8. Customer Regulatory Requirements

8.1. Customer agrees that it is solely responsible for: (i) determining whether or not Relevant Laws impose any restrictions or requirements on any of its activities in connection with this Customer Agreement and the Customer Terms (if applicable), Customer Services or any Solution; (ii) determining what Regulatory Approvals are required for Customer to use any Solution (if applicable); and (iii) as applicable, obtain from the appropriate government agencies all applicable Regulatory Approvals.

9. Warranty

9.1. Solution is provided “as is”. Except to the extent prohibited by Relevant Laws, or to the extent any statutory rights apply that cannot be excluded, limited or waived, Company, its Affiliates and its Licensors disclaim any and all representations and warranties of any kind, whether express, implied, statutory or otherwise, and shall not have any liability (whether in contract, tort, under statute or indemnities or otherwise, including negligence or fundamental breach) with respect to: (i) merchantability, fitness for purpose, non-infringement, satisfactory quality, accuracy, quality, completeness, timeliness, responsiveness, productivity, sufficiency or suitability of any Solution and relevant services, or any other matter pertaining to this Customer Agreement; (ii) Customer’s use of Solution for whatever purpose or whether any such use would comply with the regulatory requirements under the Relevant Laws or required by the government agency; (iii) reviewing the Customer Data for accuracy; (iv) any third party products or services; or (v) any application of results obtained from the use of Solution or for unintended or unforeseen results obtained in the use of Solution.

9.2. Customer acknowledges and agrees that Solution, and the access to and use thereof, may be subject to limitations, delays and other problems not in Company’s control (including such limitations, delays and other problems of or attributable to the data source) and inherent in the use of the Internet and electronic communications, and that Company shall not be held responsible for delays, delivery failures or other damage resulting from such limitations.

9.3. Customer acknowledges and agrees that Solution is designed to be a tool to assist Customer in the provision of the Customer Services, and that Company makes no warranties nor shall Company have any liability that Solution shall meet all of Customer’s requirements, or that the use of Solution shall be uninterrupted, error free or free from security defects or harmful components, or that any Data will not be lost or corrupted.

10. Liability; Indemnification

10.1. TO THE MAXIMUM EXTENT PERMITTED UNDER RELEVANT LAWS, UNDER NO CIRCUMSTANCES SHALL COMPANY BE LIABLE TO CUSTOMER FOR ANY DIRECT DAMAGES, LOSS OF PROFITS, SAVINGS, REVENUE, DATA, BUSINESS, OPPORTUNITY, REPUTATION OR GOODWILL, OR FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES OF WHATEVER NATURE FOR ANY MATTER RELATING TO SOLUTION, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT (INCLUDING UNDER ANY INDEMNITY), TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE OR STRICT LIABILITY), UNDER ANY STATUTE OR OTHERWISE, AND EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. COMPANY SHALL HAVE NO LIABILITY UNDER ANY PROVISION OF THIS CUSTOMER AGREEMENT, WHETHER IN CONTRACT, NEGLIGENCE, BREACH, OR ON ANY OTHER BASIS, WITH RESPECT TO ANY PERFORMANCE PROBLEM, CLAIM OF INFRINGEMENT OR OTHER MATTER TO THE EXTENT ATTRIBUTABLE TO ANY UNAUTHORISED OR IMPROPER USE BY CUSTOMER OR THE END USERS OF SOLUTION OR ANY BREACH OF THIS CUSTOMER AGREEMENT BY CUSTOMER.

10.2. NOTWITHSTANDING THE FOREGOING, IF COMPANY IS FOUND LIABLE DIRECTLY TO CUSTOMER FOR ANY DAMAGES, ITS TOTAL LIABILITY ON THE BASIS OF CONTRACT (INCLUDING UNDER ANY INDEMNITY), TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE OR STRICT LIABILITY), UNDER ANY STATUTE OR OTHERWISE RELATED TO, IN CONNECTION WITH AND RISING FROM ITS PROVISION OF SOLUTION SHALL NOT EXCEED THE AMOUNT EQUAL TO THE LOWER OF (A) USD $500,000 OR (B) FEES PAID BY CUSTOMER FOR ACCESS TO AND USE OF SOLUTION IN THE PRECEDING SIX (6) MONTHS PRIOR TO THE MONTH IN WHICH THE RELEVANT CLAIM IS FIRST MADE GIVING RISE TO LIABILITY; EXCEPT THAT, FOR SOLUTION PROVIDED FREE OF CHARGE, COMPANY'S LIABILITY IS LIMITED TO DIRECT DAMAGES UP TO USD TEN ($10). THE EXISTENCE OF MORE THAN ONE CLAIM OR CAUSE OF ACTION WILL NOT ENLARGE THE FOREGOING LIMIT.

10.3. Customer acknowledges that Solution is hosted on a third-party cloud hosting environment, and that Company shall not be responsible for any Losses Customer, or its End Users, may suffer or incur in connection with the use of that cloud hosting environment.

10.4. Customer agrees to indemnify, defend and hold harmless Company and its relevant Affiliates against all Losses arising from:

(a) Customer's use of Solution, including provision of the Customer Services to End Users and any other services incorporating Solution;

(b) the acts or omissions of Customer and its End Users, Affiliates, Authorised Personnel, and Representatives, or any claims by End Users in relation to the Customer Services and any other services incorporating Solution;

(c) any Security Incident of the Customer Systems or breach of any Relevant Laws;

(d) any third party claim that the following constitutes an infringement of any IP Rights of such third party: (i) Customer or its Affiliates' or Representatives' unauthorised use of Company IP or any use of any Company IP not in accordance with the terms of this Customer Agreement, or (ii) Customer's unauthorised use of Solution or its provision of any Customer Service; and/or

(e) any breach of its obligations under this Customer Agreement (which includes any schedules or addendums attached, referenced or incorporated herein, such as the applicable Solution Specific Terms, Order Forms, Data Processing Agreement, and Customer Terms (if applicable)).

11. Suspension and Downtime

11.1. Company may suspend the provision of Solution if:

(a) (i) Company reasonably believes that (A) suspension is needed to protect Solution, Company Systems supporting the Solution, or any other customer of Solution (or their end users), (B) there is unauthorized access to Solution by Customer or any End Users; or (c) suspension is required to comply with Relevant Laws; (ii) any amount due to be paid by Customer is overdue; or (iii) Customer has breached any term of this Customer Agreement (including its schedules such as the Solution Specific Terms); and

(b) Company or Reseller (if applicable) has given Customer prior written notice of its intention to suspend access to or use of Solution, in which event such action shall not give rise to any cause of breach of contract or other liability against Company.

11.2. If Company determines that any of Customer's Representatives have attempted to breach or circumvent, or have breached or circumvented, Company's security policy, Company may direct Customer to immediately terminate such Representative's access to Solution, Company Systems and / or any data contained in Company Systems (provided that, Company may terminate such access on its own if Customer fails to act upon Company's direction).

11.3. Customer acknowledges that Solution may be unavailable from time to time. Unavailability of Solution caused directly or indirectly by any of the following shall not be considered a breach by Company of this Customer Agreement (including its schedules such as the Solution Specific Terms):

(a) any problem, event or delay that is outside the reasonable control of Company (including, without limitation, a Force Majeure Event, an event that is attributable to a third party data centre that is not hosted by Company);

(b) a fault or failure of the internet or any public telecommunications network;

(c) a fault or failure of Customer's computer systems or networks;

(d) a fault or failure of devices used by End User's for accessing Solution;

(e) any breach by Customer of the Solution Specific Terms or this Customer Agreement; or

(f) scheduled, urgent or emergency maintenance, Updates carried out in accordance with this Customer Agreement or the Solution Specific Terms.

12. Charges and Payment

12.1. **Charges**. Unless otherwise stated in the Order Form, Charges will be calculated and billed monthly. Customer acknowledges that the amount billed each month may vary depending on the volume of Customer's usage of Solution. Company may bill Customer more frequently for fees accrued in Company's discretion, including if Company suspects that Customer's account may be fraudulent or at risk of non-payment. Except as otherwise expressly provided herein, all fees and Charges paid to Company are non-refundable.

If Customer purchases a resource package that includes a designated number of transactions for a specific Solution module, the transactions must be utilized within a predetermined timeframe and any unused transactions will be forfeited with no refund. In the event that all transactions are used up, Customer shall purchase an additional resource package.

12.2. **Billing.** After Customer sets up its payment method, Company will issue invoice and billing details for the previous month at the beginning of each month, which will be no later than the tenth (10th) day of each month. Company may invoice more frequently for Charges accrued if Company reasonably suspects that Customer is at risk of non-payment, or Customer's account is potentially fraudulent.

12.3. **Payment**. Customer will pay Company the applicable fees and Charges for use of Solution using one of the payment methods Company supports. Customer shall make payment in full within thirty (30) calendar days of the invoice issuance date. All amounts payable by Customer under this Customer Agreement will be paid to Company without setoff or counterclaim, and without any deduction or withholding (except on the terms of **Clause 12.8**).

12.4. **Change of Fees**. Company may increase or add new fees and Charges for Solution that Customer is using by giving Customer at least thirty (30) calendar days' prior notice. In the event that Company changes the pricing for Solution, the fees payable by Customer will increase or decrease in accordance with any such changes upon the date specified in the notice.

12.5. **Taxes**. Unless otherwise expressly specified in this Customer Agreement, all amounts due and payable by Customer to Company under this Customer Agreement or the Order Forms are exclusive of any taxes or duties imposed by Relevant Laws. Customer shall be responsible for the payment of all such taxes (including goods and services tax or other similar tax, withholding tax and indirect tax), levies, and assessments imposed upon Customer or Company arising from or in connection with this Customer Agreement. Customer shall make all payments to Company free and clear of, and without reduction for, any withholding or other taxes. Any such taxes imposed on payments to Company shall be Customer's sole responsibility, and Customer shall gross up the withholding tax to the relevant payment, ensuring that the net amount actually received by Company (free and clear of withholding tax, whether assessed against Customer or Company) shall be equal to the full amount Company would have received as if no such deduction required. Customer shall also provide Company with official receipts issued by the appropriate taxing authority, or such other evidence as Company may reasonably request, to establish that such taxes have been paid.

12.6. **Reimbursements**. Customer will reimburse Company for reasonable expenses related to providing Solution, such as the transaction fees charged by banks in the process of Customer's payment to Company.

12.7. **Late Payments**. If Customer does not pay an invoice by the due date, a late payment fee shall be applied to any such outstanding amount. Without prejudice to Company's right to termination pursuant to this Customer Agreement, Company may elect to charge Customer interest at the rate of one point five percent (1.5%) per month (or the highest rate permitted by Relevant Laws, if less) on all late payments.

12.8. **Purchase through Resellers**. Notwithstanding the provisions herein, if Customer purchases Solution through any Reseller, the payment terms between Customer and Reseller shall apply.

13. Term and Termination

13.1. This Customer Agreement shall commence on the Effective Date and will remain in effect until terminated in accordance with this Customer Agreement or applicable Order Form(s) ("**Term**"). If there is no Order Form currently in effect, either Party may terminate this Customer Agreement upon written notice to the other Party. Each Order Form will terminate upon expiry of the term under each applicable Order Form, unless expressly stated otherwise therein or in this Customer Agreement.

13.2. Termination for Cause by Company. Without prejudice to any other rights that Company may have under the Customer Terms (if applicable) as a third-party beneficiary, Company shall have the right to terminate this Customer Agreement (including all related Order Forms) or suspend Customer's access to and use of Solution immediately by notice, and terminate or suspend all licences granted to Customer immediately by notice, without any liability to Customer if:

(a) Customer (including its Authorised Personnel, End Users, Affiliates or Representatives) had used or is using Solution outside the scope of this Customer Agreement (including applicable Solution Specific Terms as incorporated herein), relevant Order Form(s) or the Customer Terms (if applicable);

(b) Customer (including its Authorised Personnel, End Users, Affiliates or Representatives) is or had been otherwise in material breach of Relevant Laws (including Relevant Laws or regulations about Personal Data, data privacy, anti-money laundering, sanctions, export or import control prohibitions in relation to technology (encrypted or otherwise), or is or had been otherwise in breach of this

Customer Agreement and has failed to cure such breach within thirty (30) days from receipt of written notice by Company; or

(c) a Security Incident has occurred with respect to Data that is in the possession of or under the control of Customer, or a change in law has occurred as set out in **Clause 18.5** below.

13.3. Upon the effective date of termination or expiry, Customer shall (i) immediately stop accessing and using Solution, delete the APIs and SDKs from Customer Systems, and (ii) where applicable, return to Company or, if required by Company, destroy all information concerning Solution in Customer's possession or control and provide written confirmation to Company confirming that all information has been returned or destroyed (as the case may be). Any amounts due and payable by Customer under this Customer Agreement shall continue to remain due and payable to Company in full immediately.

14. Data Privacy

14.1. If and to the extent applicable, Company agrees to comply with the obligations set out at in a separate Data Processing Agreement, with regards to the processing of Personal Data received from Customer ("**Transferred Personal Data**").

15. Confidentiality

15.1. Each Party retains all ownership rights in and to its Confidential Information. The Receiving Entity will use the same degree of care that it uses to protect the confidentiality of its own confidential information (but not less than reasonable care) to (i) not use any Confidential Information of the Disclosing Entity for any purpose outside the scope of this Customer Agreement and (ii) except as otherwise authorized by the Disclosing Entity in writing, limit access to Confidential Information of the Disclosing Entity to those of its and its Affiliates' employees and contractors who need that access for purposes consistent with this Customer Agreement.

15.2. The Receiving Entity acknowledges that disclosure of Confidential Information would cause substantial harm for which damages alone would not be a sufficient remedy, and therefore that upon any such disclosure by the Receiving Entity, the Disclosing Entity will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law.

16. Governing Law & Dispute Resolution

16.1. This Customer Agreement shall be governed by, and construed in accordance with, the laws of the Republic of Singapore.

16.2. Any dispute arising out of or in connection with this Customer Agreement, applicable Order Forms, Solution Specific Terms and/or Customer Terms (if applicable) and any other terms incorporated therein, including any question regarding its application, validity or termination ("**Dispute**"), shall be referred to, and exclusively and finally resolved by, arbitration administered by the Singapore International Arbitration Centre ("**SIAC"**) in accordance with the SIAC Arbitration Rules for the time being in force ("**Rules**"), which Rules are deemed to be incorporated by reference in this clause. The arbitral tribunal shall consist of three (3) arbitrators, of which one (1) arbitrator shall be appointed by Company, one (1) arbitrator shall be appointed by Customer and the third and presiding arbitrator shall be appointed by the first two (2) arbitrators as agreed between them or failing agreement within thirty (30) days from the appointment of the second arbitrator, by the President of SIAC in accordance with the Rules. The venue and seat of the arbitration must be Singapore, and the arbitration must be conducted in English.

16.3. Each Party acknowledges and agrees that a breach or threatened breach of this Customer Agreement by the other Party may cause irreparable harm and significant injury and that damages may not be a sufficient remedy in respect of such harm. Each Party may seek specific performance or injunctive or other relief as a remedy for any breach or threatened breach of this Customer Agreement by the other Party, in addition to other rights and remedies available at law or in equity.

17. Third Party Rights

17.1. The rights and protections conferred on Company under this Customer Agreement and the terms incorporated herein, shall be in addition to the rights and protections conferred on Company under any other contracts that Company has been conferred rights and protections as a third-party beneficiary. Nothing in this Customer Agreement shall limit or otherwise affect the freedom of Company or any of its Affiliates to contract with any other parties for the provision of Solution.

17.2. Customer agrees that: (i) in respect of terms in the Customer Terms (if applicable) that are intended to be for the benefit of Company, Company shall have the right to enforce directly against Customer, notwithstanding that Company is not a party to the Customer Terms (if applicable), under the Contracts (Rights of Third Parties) Act 2001; and (ii) should any dispute arise between Customer and Reseller (if applicable) under the Customer Terms (if applicable), Customer agrees to release Company from all claims, demands and damages of every kind and nature, known and unknown, suspected and unsuspected, disclosed and undisclosed, foreseeable or unforeseeable, arising out of or in any way connected to such disputes.

17.3. Unless stated otherwise in this **Clause 17**, the terms and provisions of this Customer Agreement are intended solely for the benefit of each Party and their respective successors and assigns, and it is not the intention of the Parties to confer third-party beneficiary rights upon any other Person.

18. Miscellaneous

18.1. **Further Assurance**. Each Party shall execute documents and perform acts as the other Party may reasonably require to give full effect to the provisions of this Customer Agreement, the Order Form(s) and the transactions contemplated by them.

18.2. **Legal Compliance.** Each Party shall comply, and procure that its Affiliates and Representatives (and in respect of Customer, its End Users) to comply, at all times with Relevant Laws and any lawful request of a government agency, and shall not at any time engage in any act or practice that would contravene any anti-bribery, anti-money laundering and counter-terrorist financing and sanctions statutes or regulations or any similar requirements under any Relevant Laws.

18.3. **Export Compliance**. To the extent that the performance of Company and/or Customer under this Customer Agreement is subject to any governmental restrictions or Relevant Laws on exports and/or imports, disclosures of technologies to foreign persons, exports of the same and/or derivative products thereof ("**Trade Laws**"), the relevant Party shall comply, at its sole expense, with all applicable Trade Laws (including all licensing, authorization, documentation and reporting requirements), and shall each use its commercially reasonable efforts to obtain and maintain all necessary approvals for its own activities required by the applicable government agencies. Customer shall also ensure that its use of Solution is in compliance with Company's applicable export compliance policy set out in **Schedule 2** (as may be updated by Company from time to time).

18.4. **Force Majeure**. Neither Party, nor its respective Affiliates or Representatives, shall be held liable for any default, delay or failure in performing its obligations under this Customer Agreement resulting directly or indirectly from a Force Majeure Event. A Party affected by a Force Majeure Event shall use all commercially reasonable efforts to remove or limit the effects of the Force Majeure Event, provide written notice to the other Party within ten (10) days after the occurrence of a Force Majeure Event, and re-commence performing the suspended obligations as soon as reasonably possible. If a Force Majeure Event (other than a change in law) continues for more than six (6) months, either Party may terminate this Customer Agreement by giving thirty (30) days' written notice to the affected Party.

18.5. **Change in Law.** Notwithstanding **Clause 18.4**, where Company reasonably determines that compliance with this Customer Agreement would or is likely to cause Company or any of its Affiliates to violate any Relevant Law as a result of a change in law, or any change in law makes it unlawful, impossible, or impracticable for Company to continue this Customer Agreement, as it becomes known to Company, Company may immediately suspend or terminate this Customer Agreement, in part or in full, by fifteen (15) days' prior written notice to Customer.

18.6. **Assignment**. Company is entitled to assign, transfer or novate at its sole discretion any of its rights, interest, benefits and/or obligations under this Customer Agreement (in whole or in part) without the consent of Customer, and shall provide Customer with a written notice of any such assignment, transfer or novation.

18.7. **Publicity and Media Releases.** Customer acknowledges and agrees that neither it nor any of its Affiliates or Representatives shall, without the prior written approval of Company (which Company may withhold in its sole and absolute discretion), publicise or authorise the publication of any information or issue any public announcement or press release concerning Company, any Affiliates or Representatives of Company, the existence or the contents of any Order Form, or details of Solution provided hereunder.

18.8. **Entire Agreement**. This Customer Agreement and any schedules or addendums attached, referenced or incorporated herein (including to the extent applicable the Order Form(s), Solution Specific Terms, Data Processing Agreement, and/or Customer Terms (as applicable)) constitute the entire agreement between the Parties with respect to the subject of this Customer Agreement. No provision of this Customer Agreement or a right created hereunder may be waived or varied except in writing, signed by the Parties to be bound.

18.9. **Implied Waiver.** The waiver by a Party of a breach or default by the other of any provision of this Customer Agreement, or the failure on the part of either Party to exercise any right or privilege, shall not be construed as a waiver of any subsequent breach or default by the other Party, or as a waiver of any such provision, right, or privilege.

18.10. **Notices.** Any notice or other communication in connection with this Customer Agreement shall be given in English in writing, and (i) in the case of Customer, sent to the notification email address set out in each relevant Order Form or as otherwise provided to Company or Reseller (as applicable), and (ii) in the case of Company, sent to its registered address. Customer is solely responsible for keeping its notification email address current throughout the Term.

18.11. **Invalidity and Severability.** If any provision in this Customer Agreement shall be held to be illegal, invalid or unenforceable, in whole or in part, the provision shall apply with whatever deletion or modification is necessary so that the provision is legal, valid and enforceable and gives effect to the commercial intention of the Parties. To the extent it is not possible to delete or modify the provision, in whole or in part, then such provision or part of it shall, to the extent that it is illegal, invalid or unenforceable, be deemed not to form part of this Customer Agreement and the legality, validity and enforceability of the remainder of this Customer Agreement shall, subject to any deletion or modification made not be affected.

18.12. **Nature of Relationship.** Nothing in this Customer Agreement shall be construed as creating an agency, joint venture, distributorship, franchise, commercial agency, fiduciary or employment relationship among or between Company and Customer, and neither Party has any right, power or authority to act or to create any obligation, express or implied, on behalf of the other.

18.13. **Interpretation**. In this Customer Agreement, unless a contrary intention is expressed: headings are for reference only and do not affect the interpretation of the document; the singular includes the plural and the plural includes the singular; a reference to a document (including this Customer Agreement) or legislation includes all amendments or supplements to, or replacements or novation of, that document or legislation, and in the case of legislation, all delegated legislation made under it; any reference to this Customer Agreement shall include this Customer Agreement, applicable Order Form(s), and its schedules attached hereto; a reference to a Party to any document includes that Party's successors and permitted assigns; a provision of this Customer Agreement may not be construed adversely to Company solely on the ground that Company was responsible for the preparation of this Customer Agreement or the preparation or proposal of that provision; the words "include", "including", "for example", "such as" or any form of those words or similar expressions do not limit what else is included and must be construed as if they are followed by the words "without limitation" or "but not limited to"; and a reference to "USD", "$" or "dollars" is a reference to the lawful currency of the United States.

Schedule 1 Definitions

“**Affiliate**” means in relation to a party any person directly or indirectly Controlling, Controlled by, or under common Control with that party. For the purposes of this definition, "**Control**," "**Controlling**," and "**Controlled**" mean having the right to elect a majority of the board of directors or other comparable body responsible for management and direction of a person by contract, by virtue of share ownership or otherwise.

“**API**” means any application programming interface provided by Company (via Reseller or directly) to Customer from time to time for accessing Solution.

“**Authorised Personnel**” means an employee, agent, contractor, consultant, supplier or other personnel, who is authorised by Customer to use Solution for facilitating the provision of Customer Services.

“**Business Day**” means a day other than a Saturday, Sunday or public holiday in the Territory, the People’s Republic of China, or Singapore.

“**Charges**” means the charges payable by Customer to Company in consideration for the use of Solution which are set out in this Customer Agreement and/or relevant Order Form(s).

“**Company IP**” means all IP Rights subsisting in Solution (including Updates, if any), the Documentation, and Company Systems.

“**Company Systems**” means the software (including any API and SDK), hardware, systems and network infrastructure used by Company and its Affiliates in their respective businesses, including equipment and networks connected to Solution.

“**Confidential Information**” means all information (whether oral, written or in another form) disclosed by the Disclosing Entity to the Receiving Entity, directly or indirectly, that is marked as or instructed to be confidential, or could reasonably be expected to be confidential; but does not include information which: (i) the Disclosing Entity specifies in writing is not confidential; (ii) has been duly received by the Receiving Entity from a third party which, to the knowledge of the Receiving Entity, is not subject to a confidentiality obligation to the Disclosing Entity; (iii) is or becomes part of the public domain (other than through breach of either the Customer Agreement); or (iv) was independently developed by the Receiving Entity, without reliance on any Confidential Information of the Disclosing Entity.

“**Customer**” means the legal entity that has been approved by Company to purchase Company’s Solution directly from Company or through Reseller for download, installation, access to and/or use.

“**Customer Data**” means any and all data entered or stored in, generated by or Processed by Customer in connection with Solution, including all Derived Data, De-Identified Data, and Data relating to End Users and Affiliates.

“**Customer Service**” means each product or service developed, distributed or provided by Customer (as applicable) that uses or relies on Solution.

“**Customer Systems**” means the software, hardware, systems and network infrastructure used by Customer to provide Customer Services, and otherwise used in its respective businesses, which for the avoidance of doubt excludes the Company Systems.

“**Customer Terms**” means the terms and conditions governing Customer’s purchase of Company’s Solution from Reseller (if applicable).

“**Data**” means all data (including Customer Data, Personal Data, Derived Data and De-Identified Data) which is stored, Processed or created, by or on behalf of an entity in the course of the performance of obligations under this Customer Agreement, or otherwise under or in connection with this Customer Agreement.

“**De-Identified Data**” means data derived from End User Personal Data to the extent that the personally identifiable information has been removed or detached, and as a result is no longer considered Personal Data under Relevant Privacy Laws.

“**Derived Data**” means data, in electronic or any other format, that is transformed, translated, modified, or otherwise derived from original information or data by a Party or its Affiliates. For purposes of clarity, Derived Data may be derived by transforming, translating or modifying Data, but such transformation, translation, or modification shall not affect the rights or obligations of the Parties with respect to any of the original Data.

“**Disclosing Entity**” means the entity disclosing Confidential Information, and includes that entity’s Representatives and Affiliates.

“**Dispute**” has the meaning given to that term in **Clause 16.2** of this Customer Agreement.

“**Documentation**” means documentation provided by provided by Company or its Affiliates to Customer or by Reseller to Customer, which describes the functions and use of Solution.

“**Effective Date**” is the date which is the earliest of (i) the effective date of the first applicable Order Form, (ii) when Customer first accesses or uses any Solution, or (iii) if applicable, when Customer checks a button or box confirming that Customer agrees with the terms of this Customer Agreement (e.g., “I agree to the Customer Agreement”, “Accept”, “OK” or similar).

“**End User**” means a natural person or legal entity permitted by Customer to use the Customer Services.

“**Force Majeure Event**” in relation to an entity, means an act of nature, force or cause beyond an entity’s, its Affiliates’ or Representatives’ reasonable control, including: (i) a fire, flood, elements of nature or other acts of God; (ii) pandemic or epidemic; (iii) an outbreak of escalation of hostilities, war, riots or civil disorders, or an act of terrorism; (iv) internet failures, computer, telecommunications, electrical power failures or any other equipment failures; (v) a labour dispute (whether or not employees’ demands are reasonable or within the entity’s power to satisfy); (vi) acts or omissions of a government agency prohibiting or impeding the affected entity (or its Affiliates or Representatives) from performing its obligations under this Customer Agreement, including orders of domestic or foreign courts or tribunals, governmental restrictions, sanctions, or change in law; and (vii) the non-performance by a third party for any similar cause beyond the reasonable control of the entity.

“**IP Rights**” means any of the following rights in any jurisdiction anywhere in the world: (i) all patents and patent disclosures, utility model, design patents and rights in inventions; (ii) trademarks, service marks, logos, tradenames, trade dress and domain names, together with all goodwill associated therewith; (iii) copyrights, copyrightable rights, moral rights and database rights; (iv) rights in know-how, confidential information, trade secrets, and proprietary rights and processes; and (v) all other intellectual property rights or forms of protection, subsisting now or in the future, having equivalent or similar effect to the rights referred to in any of the foregoing items (i) to (iv), subject matter of any of the foregoing, tangible embodiments of any of the foregoing, in each case, whether unregistered or registered (including all applications, rights to apply and rights to claim priority), including all divisionals, continuations, continuations-in-part, reissues, extensions, re-examinations, renewals and extensions thereof, as applicable.

“**Loss**” means all claims, judgments, awards, damages, losses, liabilities or costs of any kind and however arising, including legal costs (on a full indemnity basis), penalties, fines and interest.

“**Military End Use**” or “**Military End User**” has the meaning defined under § 744.17 and § 744.21 of the Export Administration Regulations (“**EAR**”) (or the equivalent laws of other countries and jurisdictions in the Territory).

“**Person**” includes any natural person, individual, firm, company, partnership, joint venture, an unincorporated body or association, trust, corporation or other body corporate and any government agency (whether or not having a separate legal personality).

“**Personal Data**” means: (i) information, whether true or not, about an individual who can be identified from that piece of data or from other data to which the data recipient has or is likely to have access; or (ii) considered to be personal data, personal information, personally identifiable information or equivalent under Relevant Privacy Laws.

“**Process**” (including its correlative meanings, “**Processing**” and “**Processed**”) means: (i) the receipt, access, acquisition, collection, compilation, use, modification, storage, processing, safeguarding, security, disposal, destruction, disclosure, or transfer of Data; or (ii) such other activities that may be considered to be processing of Data under Relevant Laws.

“**Prohibited Activities**” means activities that may disrupt international peace and security, including: (i) the design, development, production, handling, operation, maintenance, storage, detection, identification, dissemination or use of weapons of mass destruction, including nuclear, chemical or biological weapons; (ii) the development, production, maintenance or storage of missiles which are capable of delivering any such weapon; (iii) the transportation of any such or similar weapons; or (iv) the involvement in any military activities.

“**Receiving Entity**” means the entity receiving the Confidential Information, including its Representatives and Affiliates.

"**Regulatory Approvals**" means all permits, certificates, certifications, approvals, registrations, authorizations, and licenses which are required now or in the future for Customer and its Affiliates to use Solution in accordance with this Customer Agreement and Relevant Laws, and to meet its obligations under this Customer Agreement including where applicable the provision by Customer of the Customer Services.

“**Relevant Data Consents**” means consents or permissions given by End Users in relation to the Processing of their Personal Data.

“**Relevant Laws**” means any applicable law, statute, rule, regulation, directive, treaty, judgement, order, guidelines, decree, interpretation, permit, injunction of any government agency, whether or not of the Territory, and in each case, as amended from time to time.

“**Relevant Privacy Laws**” means Relevant Laws relating to privacy and data protection, including the PDPA and those relating to the Processing of Personal Data. Relevant Privacy Laws may refer to all privacy, personal data, and data security legislation, along with any other legislation (including regulations and directives) applicable to the Processing carried out in accordance with this DPA, including national legislation and EU legislation, as amended or replaced from time to time and different privacy and data protection regulations of different countries and regions on a case-by-case basis.

“**Representative**” of a Person means an officer, director, employee, agent, auditor, adviser, consultant, joint venturer, contractor or sub-contractor of the Person or of an Affiliate of that Person, or any other Person solely when acting at the direction of or on behalf of that Person in connection with the performance of that Person’s obligations under this Customer Agreement and/or use of Solution.

“**Reseller**” means the authorised reseller of Company that enters into the Customer Terms with Customer in relation to Customer’s use and access of Solution.

“**Reseller Agreement**” means the agreement entered into by Company and Reseller (if applicable) which sets out the terms and conditions governing Reseller’s promotion and resale of Company’s Solution to Customer.

“**Rules**” has the meaning given to it in **Clause 16** of this Customer Agreement.

“**Sanctioned Person**” means (i) a Person who appears on the list of Specially Designated Nationals and Blocked Persons maintained by the U.S. Department of the Treasury, the Office of Foreign Assets Control, or any other list of Persons with whom dealings are restricted or prohibited by the laws of the Republic of Singapore, the United States, the People’s Republic of China, the United Kingdom, the European Union, or the United Nations, and any other jurisdiction which may apply to any transactions and / or dealings involving Customer to which this Customer Agreement directly or indirectly applies to (collectively "**Relevant Jurisdictions**"), (ii) the government agency of any country against which any Relevant Jurisdiction maintains comprehensive economic sanctions or embargos, (iii) a national or resident of any country against which any Relevant Jurisdiction maintains comprehensive economic sanctions or an embargo, or (iv) a Person acting or purporting to act, directly or indirectly, on behalf of, or a Person owned or controlled by, any of the Persons listed in (i) to (iii) above.

"**SDK**" means any software code provided by Company to Customer from time to time, for incorporation by Customer into any Customer Systems to enable the relevant devices to call, invoke, redirect to, communicate with, or otherwise access Solution.

"**Security Incident**" means any actual or suspected: (i) loss or misuse of Personal Data by any means; (ii) unauthorised or unlawful Processing, sale, or rental of Personal Data, including under Relevant Laws and Relevant Data Consents; or (iii) other act or omission that compromises the privacy, security or confidentiality of Personal Data.

"**SIAC**" has the meaning given to it in **Clause 16** of this Customer Agreement.

"**Solution**" means Company's products and services purchased by Customer directly from Company or from Resellers, as customised, modified or amended from time to time.

"**Solution Specific Terms**" means the terms and conditions between Company and Customer, governing Customer's download, installation, access to and/or use of the relevant Solution, as amended or updated by notice in writing from Company to Customer directly or to Reseller from time to time.

"**Term**" has the meaning given to that term in **Clause 13.1** of this Customer Agreement.

"**Territory**" means the territory within which, Company has approved, for Customer to purchase (from Company or Reseller, if any) and thereafter, download, install, access to and/or use of any of Solution.

"**Trade Laws**" has the meaning given to that term in **Clause 18.3** of this Customer Agreement.

"**Transferred Personal Data**" has the meaning given to it in **Clause 14** of this Customer Agreement.

"**Updates**" means modifications to Solution provided by Company from time to time.

Schedule 2 Export Compliance Policy

1 Trade Control Laws

1.1 Company is committed to fully comply with Singapore Strategic Goods (Control) Act and all applicable Trade Laws governing the export, re-export, import, in-country transfers, transit, and trans-shipment of Solution and related products, software, services, support and technology.

2 Export Compliance Policy

2.1 Solution is subject to export and import controls administered by the Singapore government and other countries (including the United States, United Kingdom, the member states of the European Union, and other foreign jurisdictions), including in particular the following prohibitions:

(a) export, re-export or transfers in violation of Trade Laws of Singapore, the United States, the United Kingdom or the European Union, or other applicable laws and regulations;

(b) export, re-export or transfers, either directly or indirectly, to Cuba, Iran, North Korea, Syria, the Crimea, Luhansk, Donetsk regions of Ukraine, and any other country or region subject to export control sanctions;

(c) export, re-export, or transfer (in-country) for use in connection with military end use, military end user, or weapons of mass destruction;

(d) use of Solution to facilitate cybersecurity or network disruption, monitoring or tracking that could assist in or enable human right abuses.

3 Sanction Compliance Policy

3.1 Trade Laws prohibit or restrict unauthorised transactions with Sanctioned Persons (including parties identified as engaging in terrorism, narcotics trafficking, weapons proliferation, and other activities that threaten national security, stability, or foreign policies).

3.2 In order to comply with the applicable Trade Laws, it is Company's general policy that Solution is **prohibited** from transacting with parties that are sanctioned by applicable authorities (including authorities of Singapore, the United States, the People's Republic of China, the United Kingdom, the European Union, and the United Nations), as well as parties located in the following territories:

(a) Cuba

(b) Iran

(c) North Korea

(d) Syria

(e) Crimea region, Donetsk region, Luhansk region

3.3 It is also Company's general policy that Solution is **restricted** (and is required to obtain prior internal clearance in writing) from transacting with parties located in the following territories:

(a) Russia

(b) Belarus

(c) Venezuela

(d) Myanmar

Solution Specific Terms

For eKYC Identity Verification ("Solution")

These Solution Specific Terms (these "**Solution Specific Terms**") between Company and Customer contain additional terms and conditions applicable to this particular Solution. Unless otherwise defined in these Solution Specific Terms, capitalised terms used in these Solution Specific Terms have the meaning given to them in the SaaS Solution Customer Agreement entered into between Company and Customer (the "**Customer Agreement**").

In these Solution Specific Terms:

(a) "**Average Error Rate**" means the sum of all Error Rates in all the Time Intervals in a billing period divided by the total number of Time Intervals in such billing period.

(b) "**Error Rate**" means the total number of Failed Transactions divided by the Total Transactions during each Time Interval.

(c) "**Failed Transaction**" means an attempted request to complete a transaction that reaches server but cannot be processed as read due to system error, the return result of which shows "SYSTEM_ERROR"; for the avoidance of doubt, (i) any return results that shows "REQUEST_TRAFFIC_EXCEED_LIMIT" shall not be deemed as Failed Transactions hereunder, (ii) a maximum volume of API requests Processed per second by all the Customer Services shall not exceed five (5), and if the number of the API calls per second exceeds such limit, any error return shall not be deemed as Failed Transactions hereunder, and (iii) if there is any empty field in a return result, such return result shall not be deemed as a Failed Transaction hereunder.

(d) "**Monthly Service Fee**" means the total Charges paid by Customer for Solution in one billing month. For the annual subscription fees paid by Customer for Solution, the Monthly Service Fee equals to the annual subscription fees divided by the number of months of Solution covered by such annual fees. For the lump sum prepayment, the Monthly Service Fee will be set out in the monthly invoice for Solution based on actual usage.

(e) "**Monthly Uptime Percentage**" means a percentage of Solution availability calculated by reference to the following formula:

Monthly Uptime Percentage = (1 - Average Error Rate) x 100%

(f) "**Service Credit**" means the percentage of the Monthly Service Fee for the affected Solution that is credited to Customer for a Claim following the service credit claim process under **Clause 5** of these Solution Specific Terms.

(g) "**Time Interval**" means each time interval of five (5) minutes. For the purpose of these Solution Specific Terms, if any Permitted Downtime occurs during any Time Interval, such Time Interval shall be excluded for the calculation of the total number of Time Intervals as referred to in the definition of Average Error Rate, and each Error Rate during such Time Interval where any Permitted Downtime occurs, shall be excluded from the calculation of aggregate Error Rates in all the Time Intervals in a billing period as referred to in the definition of Average Error Rate.

(h) "**Total Transactions**" means the total number of attempted requests from Customer to complete a transaction as received by server of Company.

4 Solution Service Standards

4.1 Availability Service Level

Subject to **Clause 11** of the Customer Agreement, Company shall provide a Monthly Uptime Percentage of no less than 99.95% each billing month in connection with Customer's use of Solution (the "**Service Level**"). For the avoidance of doubt, the Service Level does not apply to any unavailability, suspension, failure, or termination of the use of Solution, or any other Solution performance issues resulting from or in connection with Permitted Downtime.

For the purposes of this Service Level under this **Clause 4.1**, "**Permitted Downtime**" means:

(e) any event described in **Clause 11.3** of the Customer Agreement;

(f) any downtime caused or contributed to by any act or omission of Customer or any of Customer's Representatives or End Users otherwise than in accordance with these Solution Specific Terms; or

(g) any downtime caused or contributed to by the interaction between Solution and any End User applications using or communicating with the SDKs.

4.2 Service Standards for Incident Response

Company acknowledges and agrees that the ability of Customer to provide the Customer Services to End Users is dependent upon the connectivity and availability of Solution, APIs and SDKs (as applicable). Company shall provide the following commitments upon the occurrence of any Incident which affects the availability or provision of Solution:

Incident Severity Level	Description	Target Response Time
P0	Severe Incident: Customer cannot use critical job functions in production environment Customer's entire End User base is impacted Workaround required immediately or Solution is unavailable	Four (4) hours
P1	Major Incident: Functionality of Solution impacted A portion of Customer's End User base is impacted Workaround required	Eight (8) hours on a Business Day
P2	Incident has affected or will affect Customer's productivity: Workaround exists, but incident needs to be fixed Solution can be used and accessed, but with a level of degradation that is acceptable for Customer in the short-term	Twenty-four (24) hours on Business Days
P3	No or minimal impact on Customer: Incident does not affect Solution	Five (5) Business Days

For the purposes of the service standards under this **Clause 4.2**, an "**Incident**" means a failure of Solution to materially conform to its Documentation, but does not include a failure caused by:

(h) any event described in **Clause 11.3** of the Customer Agreement;

(i) a modification of Solution without Company's consent;

(j) a defect, error or malfunction in any item of hardware or software not supplied by Company or its Affiliates pursuant to the Customer Agreement; or

(k) API requests Processed per second by all the Customer Services exceeding five (5).

The aforementioned events and circumstances are collectively known as "**Exclusion Events**".

5 Service Claim

5.1 If Customer believes that the Service Level in connection with its use of Solution is not met, then Customer may file a claim for Service Credit in accordance with this **Clause 2** (a "**Claim**"). Such Claim must include at least the following information:

(l) a detailed description of the Incident;

(m) the dates and number of Failed Transactions, and number of transactions within the claimed month;

(n) information relating to the affected instances; and

(o) any other information that Company reasonably asks Customer to provide to support the Claim.

5.2 The Claim must be received by Company within thirty (30) days after the occurrence of the event giving rise to the Claim. Customer's failure to submit the Claim within this time shall be deemed to be an irrevocable waiver of Customer's right to the Claim and receive the relevant Service Credit. Once Company receives the Claim, Company will review and evaluate the Claim and may require Customer's co-operation in conducting a joint investigation to ascertain whether the Service Level has been breached and if so, the cause of the failure. Company will make a good faith determination if a Service Credit is to be provided to Customer in Company's sole discretion and shall inform Customer the result as soon as reasonably practicable. Company will use commercially reasonable effort to process the Claim and provide the Service Credit to Customer.

5.3 If Company, after its good faith review of the Claim, determines that a Service Credit should be provided to Customer, the Service Credit to be provided will be the following. Customer acknowledges and agrees that this is the sole and exclusive remedy for service availability.

Monthly Uptime Percentage	Service Credit
Less than 99.95%, but equal to or greater than 99%	5%
Less than 99.00%, but equal to or greater than 95%	10%
Less than 95.00%	30%

6 Miscellaneous

6.1 Company reserves the right to alter, modify, add to or otherwise vary these Solution Specific Terms by notice to Customer in such manner as Company deems appropriate. Customer shall be bound by the terms as amended. In any event, if Customer continues to use Solution after such notice, Customer shall be deemed to have accepted the amendment.

6.2 In addition to these Solution Specific Terms, Customer shall also be bound by the Order Form, the general terms under the Customer Agreement as well as such other terms and conditions as may be agreed by Customer. The rights and protections conferred on Company under these Solution Specific Terms shall be in addition to the rights and protections conferred on Company under the Order Form, the Customer Agreement, any other terms and conditions agreed by Customer, and other contracts that Company has been conferred rights and protections as a third-party beneficiary (such as the relevant Reseller Agreement).

Data Processing Agreement

This Data Processing Agreement ("**DPA**") is incorporated into and forms an integral part of the SaaS Solution Customer Agreement (the "**Customer Agreement**") entered into by and between Zoloz Pte. Ltd. ("**Company**") and Customer, both as defined in the Customer Agreement.

In the event of any conflict or inconsistency between the terms of this DPA and any terms or conditions of the Customer Agreement, the terms of this DPA shall prevail.

1 Definitions

1.1 "Personal Data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.2 "**Controller**" means an organisation which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.3 "**Data Subject**" means a natural person (i.e. individual) whose Personal Data is Processed.

1.4 "**Processor**" means an organisation which Processes Personal Data on behalf of another organisation but does not include an employee of that other organisation.

1.5 "**Relevant Laws**" means any applicable law, statute, rule, regulation, directive, treaty, judgement, order, guidelines, decree, interpretation, permit, injunction of any Government Agency, whether or not of the Territory, and in each case, as amended from time to time.

1.6 "**Relevant Privacy Laws**" means Relevant Laws relating to privacy and data protection, including the PDPA and those relating to the Processing of Personal Data. Relevant Privacy Laws may refer to all privacy, personal data, and data security legislation, along with any other legislation (including regulations and directives) applicable to the Processing carried out in accordance with this DPA, including national legislation and EU legislation, as amended or replaced from time to time and different privacy and data protection regulations of different countries and regions on a case-by-case basis.

1.7 All capitalized terms not defined in this DPA shall have the meaning set forth in the Customer Agreement.

2 Scope and Roles

2.1 This DPA applies when Company Processes any Personal Data.

2.2 Customer agrees and acknowledges that any Processing of any Personal Data by Company or its Affiliates, is carried out by them as data intermediaries, data processors or other similar designation under Relevant Privacy Laws, of Customer, on behalf of Customer and for the purposes of Customer.

2.3 Customer may be either a Controller or a Processor.

3 Customer Obligations

3.1 Customer represents and warrants to Company that it has the legal right under all Relevant Laws and has taken the proper steps to ensure that Company and/or its Affiliates are able to lawfully Process the Personal Data pursuant to the Customer Agreement and this DPA, including providing all required notices or statements to Data Subjects of the Personal Data, obtaining all required Relevant Data Consents from Data Subjects of the Personal Data, and obtaining or completing all required approvals, registrations, filings or other governmental procedures.

3.2 Customer must:

3.2.1 promptly notify Company in writing of any complaint or investigation under, or relating to, any Relevant Privacy Laws or Relevant Data Consents concerning the Customer's use of Solution or concerning the Personal Data or any circumstances that may lead to any such complaint or investigation;

3.2.2 act promptly in the resolution of any such complaint, investigation or circumstances;

3.2.3 not do, or omit to do, anything which would put Company in breach of Relevant Privacy Laws or Relevant Data Consents;

3.2.4 take all such steps as Company reasonably requires of it to facilitate Company's compliance with any of the Relevant Privacy Laws or Relevant Data Consents that apply to Company, including any Relevant Privacy Laws obliging Company to obtain Relevant Data Consents or to store a copy of Personal Data within the Territory (including in the circumstance of assignment of Company's rights under the Customer Agreement);

3.2.5 comply with Company's security requirements regarding the dedicated or direct interconnection between its systems, platforms or devices and Customer's operating environment, as specified in the Customer Agreement;

3.2.6 promptly notify Company in writing if it becomes aware of any changes to a Relevant Privacy Law that may cause the Customer Services, the Processing of Personal Data or any other activities of Company relating to the Customer Agreement, to breach such Relevant Privacy Law; and

3.2.7 Company may audit or require a copy of an internal or external audit performed in respect of Customer's compliance with this **Clause 3** from time to time.

3.3 Customer agrees that Company is not and will not be responsible for the Processing of Personal Data other than Company's Processing of Personal Data in accordance with the Customer Agreement and this DPA. Customer is solely responsible for the development, content, operation, maintenance, and Processing of Personal Data in connection with the Customer Services or the Customer Agreement, including:

3.3.1 ensuring that the Processing of Personal Data, including by Company, and/or its Affiliates, complies with the Relevant Privacy Laws, Relevant Data Consents, and other notices or disclosures provided or made;

3.3.2 any claims relating to or Losses arising from the Processing of Personal Data or a Security Incident;

3.3.3 properly handling and processing notices sent to Customer by any Person claiming that Personal Data (or any actions in relation to it, including actions consistent with the terms of the Customer Agreement) is in breach of Relevant Privacy Laws or violates such Person's rights;

3.3.4 responding to any request which Customer may receive from any End User seeking to exercise the rights over his/her Personal Data that he/she may be entitled to in accordance with the Relevant Privacy Laws; and

3.3.5 taking its own steps to maintain appropriate security, protection and backup of Personal Data, which may include the use of encryption technology to protect Personal Data from unauthorised access and appropriate archiving of Personal Data.

3.4 In processing transactions using the Services, Customer acknowledges and agrees that all Personal Data shall be provided in accordance with data standards developed and issued by Company. The data standards are published by Company or its Affiliates and may be varied by Company or its Affiliates from time to time with notice to Customer.

3.5 In relation to all Personal Data to be Processed in connection with the Customer Services, Customer must ensure that:

3.5.1 all consents or approvals required under, or are otherwise necessary or useful to comply with, Relevant Privacy Laws have been obtained;

3.5.2 all Relevant Data Consents that are necessary or useful for Company to provide the Customer Services to Customer and otherwise perform its other obligations under the Customer Agreement have been obtained;

3.5.3 all notices and disclosures that are required under, or otherwise necessary or useful to comply with Relevant Privacy Laws and Relevant Data Consents and any notices and disclosures that Customer is required to provide to Data Subjects of Personal Data or government agencies have been provided or made, including those concerning:

(i) the collection of Personal Data by, and disclosure of Personal Data to, Company or its Affiliates;

(ii) the collection and transfer of Personal Data in, by and from the Services in the course of receiving and providing the Services and Customer Services; and

(iii) the Processing of Personal Data by Company,

as contemplated by the Customer Agreement, including being consistent with and reflecting Company's status as described in **Clause 3.4**; and

3.5.4 a record of all consents (including Relevant Data Consents) or approvals in connection with this **Clause 3.5** is maintained in accordance with all Relevant Privacy Laws.

3.6 After Customer complies with the requirements of this **Clause 3**, if for any reason, whether under Relevant Privacy Laws or any requirement reasonably imposed by Company, Customer is required to subsequently obtain any consent or approval of such Data Subject of Personal Data or government agency for any Processing of Personal Data as set out above, Customer must inform Company and shall obtain such consent or approval before Processing such Personal Data which is the subject of such consent or approval.

4 Company’s Processing of Data

4.1 In respect of Personal Data, Company will comply with the Relevant Privacy Laws in relation to its Processing of Personal Data.

4.2 Company will only Process the Personal Data:

4.2.1 in accordance with Customer’s documented instructions that may be specified from time to time; or

4.2.2 as required to comply with any Relevant Laws, in which case Company shall, to the extent permitted by Relevant Laws, notify Customer as soon as reasonably practicable before complying with such law.

4.3 In the event that Company becomes aware that an instruction from Customer may, in Company’s reasonable opinion, infringe any Relevant Laws, Company shall promptly notify Customer, in which case Customer must withdraw and/or modify the relevant instruction.

4.4 Company will implement appropriate security measures set out in Appendix 2 to protect Personal Data against unauthorised or accidental access, Processing, modification, copying, disposal, destruction or similar risks.

4.5 Company will notify Customer as soon as reasonably practicable if Company receives any complaint, notice or communication (whether from a government agency or Data Subject or otherwise) which relates directly or indirectly to the Processing of Personal Data, or the exercise of any rights of the Data Subject in respect of Personal Data. Company will promptly notify Customer in writing after becoming aware of occurrence of a Security Incident affecting the Personal Data.

4.6 Company will provide reasonable assistance, information and cooperation to Customer with respect to meeting Customer's obligations under the Relevant Privacy Laws, including in relation to:

4.6.1 notifying Customer of any request received by Company from Data Subjects to exercise rights over Personal Data;

4.6.2 notification by Customer of Security Incidents to government agencies or Data Subjects; and

4.6.3 carrying out data protection impact assessments in relation to the Processing of such Personal Data, if required.

4.7 Company will either delete or return to Customer the Personal Data upon Customer's written request, after the end of the provision of Solution, or as necessary to comply with a request by a Data Subject to exercise rights over Personal Data, save that Company may continue to retain copies of or Process the Personal Data to the extent permitted by the Relevant Privacy Laws.

5 Sub-Processing

5.1 Customer hereby grants a general authorisation to Company for Company to engage sub-processors to Process Personal Data, provided that Company shall ensure that the terms on which it engages such sub-processors comply with the Relevant Privacy Laws and are consistent with the obligations imposed on Company in this DPA.

5.2 To the extent required by the Relevant Privacy Laws, Company will give Customer reasonable prior notice before its engagement of sub-processors. If within ten (10) days of Customer's receipt of such notice, Customer notifies Company in writing of any objections (on reasonable grounds associated with data protection considerations) to the proposed engagement:

5.2.1 Company may elect to make available a commercially reasonable change in the provision of Solution which avoids the use of that proposed sub-Processor; or

In the absence of any written notice from Customer expressly objecting to the proposed engagement of sub-processors, Customer shall be deemed to have consented to such engagement.

6 Location of Processing and Cross-Border Transfers

6.1 Customer acknowledges and consents that Personal Data may be Processed and stored on location(s) other than where Company is incorporated. The location(s) where Personal Data are Processed and stored shall be agreed by the Parties depending on the Solution.

6.2 Customer further consents that, with respect to use of certain Solution involving the Ant Digital Technology Official Website services, Personal Data may be transferred to the mainland of the People's Republic of China for Processing for the purpose of service maintenance.

6.3 The Parties agree to execute standard contractual clauses or any other document of similar nature as may be required by the Relevant Privacy Laws from time to time with respect to cross-border transfers of Personal Data.

6.4 For any transfer by Customer of Personal Data from (i) the European Economic Area and Switzerland and/or (ii) the United Kingdom (collectively, "**Restricted Counties**") to Company in a country or region which does not ensure an adequate level of protection (within the meaning of and to the extent governed by the Relevant Privacy Laws of the Restricted Countries), such transfer shall be governed by (i) the EU Standard Contractual Clauses and/or (ii) the UK Standard Contractual Clauses Addendum set forth in Appendix 3.

Company agrees to comply with the EU Standard Contractual Clauses and the UK Standard Contractual Clauses Addendum (as applicable) set forth in Appendix 3. For these purposes, and notwithstanding that Customer may be an organisation located outside of the Restricted Countries, Company shall be the “data importer” and Customer shall be the “data exporter” under the EU Standard Contractual Clauses and UK Standard Contractual Clauses Addendum set forth in Appendix 3.

The EU Standard Contractual Clauses and the UK Standard Contractual Clauses Addendum are hereby incorporated by reference into this DPA and shall form an integral part thereof.

7 Audit

7.1 Customer may conduct an audit no more than once a year, to verify Company’s compliance with its obligations under this DPA when necessary (e.g., requirements from supervisory authority or violation of Relevant Privacy Laws are found), by reviewing the necessary documentations made available by Company to Customer.

7.2 Company will, if required under the Relevant Privacy Laws, allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Company’s compliance with its obligations under this DPA in accordance with the following:

7.2.1 Customer demonstrates to the reasonable satisfaction of Company that such audits are required by the Relevant Privacy Laws;

7.2.2 the Parties will mutually agree upon the scope, timing, duration, and control and evidence requirements before the conducting of the audit;

7.2.3 if Customer mandates an auditor, such auditor must not operate businesses in competition with Company and has entered into a non-disclosure agreement with Company on terms acceptable to Company; and

7.2.4 to the extent permitted by the Relevant Privacy Laws, upon Company’s request, Customer is responsible for bearing all costs and fees related to such audit, including all reasonable costs and fees for any and all time Company incurs for any such audit.

7.3 For the avoidance of doubt, the exercise of audit rights under the EU Standard Contractual Clauses and UK Standard Contractual Clauses Addendum set forth in Appendix 3 shall be as described in this Clause.

8 Duration

Notwithstanding the expiry or earlier termination of the Customer Agreement, this DPA will remain in effect until the deletion or return of all Personal Data as described herein.

Appendix 1 to Data Processing Agreement

Purpose(s) of the Processing	• As necessary for Company to provide Solution under the Customer Agreement, including use of Personal Data Personal Data to improve and optimise the service quality, the functionality, and relevant algorithms and models; • With respect to use of certain Solution involving the eKYC services, Personal Data Personal Data may be transferred to the mainland of the People's Republic of China for Processing for the purpose of verifying the End User's identity on public security database, and the verification results will be stored on severs located within the mainland of the People's Republic of China and be provided to Customer.
Categories of Data Subjects whose Personal Data is Processed:	The categories of Data Subjects are determined by Customer and may include but not limited to: • End Users; • Customer's employees and workers; • Business contacts of Customer's vendors, business partners, customers, and potential customers; • For certain Solution involving the eKYB services, the senior management, shareholder, and ultimate beneficial owner of the specific company (to the extent that such shareholder or ultimate beneficial owner is an individual) that Customer requests to verify; and • For certain Solution involving the AML services, the senior management, shareholder, and ultimate beneficial owner of the customer of Customer (to the extent that such shareholder or ultimate beneficial owner is an individual).
Categories of Personal Data Processed:	Company may Process the following categories of Personal Data determined by Customer, in each case in accordance with Customer's documented instructions: • Identification, biographical and contact data (such as name, gender, nationality, birthday, education, ID number, issue/expiry date of ID document, address, phone number, email account, position, and other details); • Financial data (such as payment information, transaction information, account details); • Employment data (such as employer, employee, title, office information, responsibility); • Device information and environment information; • For certain Solution involving the eKYC services, information stored in the user's ID chip that can be read by NFC on mobile; and • For certain Solution involving the eKYB or AML services, shareholding structure and percentage information of the shareholder or ultimate beneficial owner of relevant company (to the extent that such shareholder or ultimate beneficial owner is an individual); • any other types of Personal Data that Customer or Customer's End Users transfer or upload.

	The above Personal Data may contain sensitive Personal Data or special categories of Personal Data or other similar designation under Relevant Privacy Laws, depending on the definition of Relevant Privacy Laws for that term.
Transfers to (sub-) Processors:	Please refer to a list of sub-processors made available on Company’s website at https://mdn.alipayobjects.com/huamei_dilt5f/afts/file/A*jKpWSbwkjF8AAAAAAAAAAAAADm_4AQ/SUB-PROCESSORS-LIST.pdf

Appendix 2 to Data Processing Agreement

Security Measures

Company has implemented and will maintain the following security measures to safeguard security of Transferred Personal Data, which in conjunction with the obligations in this DPA, are Company's only responsibility with respect to the security of that data.

Organization of Information Security	**Security Roles and Responsibilities**. Company's Authorised Personnel with access to Transferred Personal Data are informed of the confidential nature of the Transferred Personal Data and are bound by confidentiality obligations. **Risk Management Program**. Company performed a risk assessment before processing the Transferred Personal Data or launching the Solution.
Asset Management	**Asset Inventory**. Company maintains an inventory of all media on which Transferred Personal Data is stored. Access to the inventories of such media is restricted to Authorised Personnel. **Asset Handling** - Company applies data classification and levelled protection on Transferred Personal Data to help identify it and to allow for access to it to be appropriately restricted. - Company's Authorised Personnel must obtain Company authorization prior to storing Transferred Personal Data on portable devices, remotely accessing such data, or processing such data outside Company's facilities.
Human Resources Security	**Background Check**. Company performs a background and qualification check towards Authorised Personnel, to the extent permitted by applicable law. Authorised Personnel are required to agree to the terms of the Code of Conduct and accept related security trainings. **Security Training**. Company informs its Authorised Personnel about relevant security procedures and their respective roles. Company also informs its Authorised Personnel of possible consequences of breaching the security rules and procedures.
Physical and Environmental Security	**Physical and Logical Safeguards**. Company employs both physical and logical safeguards to ensure data is tightly controlled and limited to Authorized Personnel only. Such controls include, but are not limited to physical access restrictions; authentication security appropriate to the system and data; monitoring and logging access to systems and applications; data loss prevention tools; enforced security policies; multi-factor authentication for remote access to corporate resources; and unique, limited duration, single-use user credentials for Company's privileged accounts. **Disposal**. Company uses industry standard processes to delete Transferred Personal Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. Company maintains security documents describing its security measures and the relevant procedures and

	responsibilities of its personnel who have access to Transferred Personal Data. **Data Backup and Recovery** - Company develops back up strategy and recovery strategy for data based on the security level of the concerned data and the impact of the concerned data on system operations. - Production data is backed up in real time and offsite and takes the form of incremental backup and full backup. Incremental backup should be at least once per day and full backup should be at least once a week. - Company checks the validity of backup data at least once a quarter and periodically verifies the recovery of the backup of major business data to ensure the availability of the data. - Company establishes remote data backup and recovery functions for both co-located and offsite data backup centers, and uses communication networks to transfer critical data to the backup site on a regular basis. - Company conducts regular disaster recovery drills on an annual basis and performs validation tests on the availability of the application of key technologies. - Company has specific procedures in place governing access to copies of Transferred Personal Data. **Encryption** - Company encrypts, or enables Customer to encrypt, Transferred Personal Data that is transmitted over public networks. - Company restricts access to Transferred Personal Data in media leaving its facilities. **Event Logging**. Company logs, or enables Customer to log, access and use of information systems containing Transferred Personal Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Company maintains a record of security privileges of individuals having access to Transferred Personal Data. **Access Authorization** - Company maintains and updates a record of Authorised Personnel authorized to access Company systems that contain Transferred Personal Data. - Company identifies those personnel who may grant, alter or cancel authorized access to data and resources. **Least Privilege**. Access to Company systems is based on the principle of "least privilege," and Authorised Personnel are given the minimum access required to perform their duties. Access is valid only for the duration necessary for Authorised Personnel to complete applicable tasks. Access is further restricted based on separation of duties.

	Authentication - Company uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Company requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Company requires the password to be at least eight characters long. - Company ensures that de-activated or expired identifiers are not granted to other individuals. - Company monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Company maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Company uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.
Information Security Incident Management	**Incident Response Process** - Company maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Company will be made without undue delay. - Company tracks, or enables Customer to track, disclosures of Transferred Personal Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Company security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Company maintains emergency and contingency plans for the facilities in which Company information systems that process Transferred Personal Data are located. - Company’s redundant storage and its procedures for recovering data are designed to attempt to reconstruct Transferred Personal Data in its original or last-replicated state from before the time it was lost or destroyed. - Company review security measures at least annually to ensure that it protects the availability, integrity, and confidentiality of Transferred Personal Data.

Appendix 3 to Data Processing Agreement

EU Standard Contractual Clauses and UK Standard Contractual Clauses Addendum

1 Definitions

1.1 "**EU Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to third countries approved pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 available at here.

1.2 "**UK Standard Contractual Clauses Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, in force from March 21, 2022, available at here.

1.3 The terms "Controller", "Data Subject", and "Processor" shall have the same meaning given to them or correlative terms under applicable Relevant Privacy Laws.

2 EU Standard Contractual Clauses

For transfer of Personal Data out of the European Economic Area or Switzerland subject to **Clause 6.4** of this DPA, the EU Standard Contractual Clauses are incorporated into this DPA by reference in the following manner:

2.1 Module Two (Controller to Processor) shall apply to the extent Customer is a Controller and Module Three (Processor to Processor) shall apply to the extent Customer is a Processor;

2.2 The optional Clause 7 is excluded;

2.3 For the Clause 9(a), Option 2 (General Written Authorisation) is selected, and the time period for prior notice of sub-Processor changes is set forth in **Clause 5** of this DPA;

2.4 For the Clause 11(a), the option paragraph is excluded;

2.5 For the Clause 17, Option 1 is selected, and the EU Standard Contractual Clauses shall be governed by the law of Ireland;

2.6 For the Clause 18, the dispute shall be resolved before the courts of Ireland;

2.7 For Part A of Annex I, the following shall apply:

a) Data exporter: The entity identified as "Customer" in the Customer Agreement;

Contact information: the email address associated with Customer's account;

Activities relevant to the data transferred under these Clauses: The data importer provides Solution to the data exporter in accordance with the Customer Agreement.

Role: As outlined in **Clause 2** of this DPA; and

Signature & Date: The date when Customer clicks a box indicating acceptance to the Customer Agreement (e.g., I agree to the Customer Agreement, or similar button), or execute an order form that references the Customer Agreement, or use free services provided by Company.

b) Data importer: Company (as defined in the Customer Agreement);

Address: as specified in the Customer Agreement:

Contact information: as provided under the "Notices" section of the Customer Agreement;

Activities relevant to the data transferred under these Clauses: The data importer provides Solution to the data exporter in accordance with the Customer Agreement.

Role: As outlined in **Clause 2** of this DPA; and

Signature & Date: The date when Customer clicks a box indicating acceptance to the Customer Agreement (e.g., I agree to the Customer Agreement, or similar button), or execute an order form that references the Customer Agreement, or use free services provided by Company.

2.8 For Part B of Annex I, the description of the transfer is as described in Appendix 1 (Description 0f Transfer);

2.9 For Part C of Annex I, the competent supervisory authority/ies shall be determined according to the General Data Protection Regulation and Clause 13 of the EU Standard Contractual Clauses;

2.10 For Annex II, Appendix 2 states the technical and organizational security measures implemented by the data importer;

2.11 For Annex III, the Controller has authorised the use of the sub-Processor(s) listed in Appendix 1; and

2.12 Where the Transfer relates to Personal Data governed by the laws of Switzerland, the Parties agree that:

a) All references in the 2021 SCCs to "EU," "Union" or "Member State" will be interpreted as references to Switzerland and all references in the EU Standard Contractual Clauses to provisions in EU law will be interpreted as references to the relevant provisions of the laws of Switzerland;

b) For the purpose of Clause 17 of the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be governed by the laws of Switzerland;

c) For the purpose of Clause 18 of the EU Standard Contractual Clauses, any dispute arising from the EU Standard Contractual Clauses will be resolved by the courts of Switzerland; and

d) For the purpose of Part C of Annex I of the EU Standard Contractual Clauses, the competent supervisory authority is the data protection authority of Switzerland.

3 Mutual Understanding regarding EU Standard Contractual Clauses

3.1 The Parties agree that each of the following forms an integral part of the EU Standard Contractual Clauses and set out the mutual understanding of their respective obligations under the EU Standard Contractual Clauses:

a) For Clause 8.9 of the EU Standard Contractual Clauses, Customer acknowledges and agrees to exercise audit right under the respective clause according to **Clause 7** of this DPA;

b) For Clause 9(c) of the EU Standard Contractual Clauses, Customer acknowledges and agrees that Company may be restricted from providing sub-Processor agreement(s) due to confidentiality obligation; and

c) For Clause 12 of the EU Standard Contractual Clauses, Customer acknowledges and agrees that any liability and claims arising from the Standard Contractual Clauses shall be in accordance with and to the limitation set forth in the Customer Agreement.

4 UK Standard Contractual Clauses Addendum

4.1 For transfer of Personal Data out of the United Kingdom subject to **Clause 6.4** of this DPA, the UK Standard Contractual Clauses Addendum is incorporated into DPA by reference in the following manner:

a) The applicable version of the EU Standard Contractual Clauses appended to this DPA shall apply for the purposes of Table 2 of the UK Standard Contractual Clauses Addendum;

b) The provisions of the UK Standard Contractual Clauses Addendum, including Part 2 'Mandatory Clauses', shall apply in full and are hereby incorporated by reference to this DPA;

c) Table 1 of the UK Standard Contractual Clauses Addendum, the names of the parties, their roles and their details shall be considered populated by the information set out in Annex I of the EU Standard Contractual Clauses;

d) Tables 2 and 3 of the UK Standard Contractual Clauses Addendum shall be considered populated by the applicable version of the EU Standard Contractual Clauses as appended to this DPA, including the information set out in the Annexes of the EU Standard Contractual Clauses; and

e) For the purposes of Table 4 of the UK Standard Contractual Clauses Addendum, neither Party may end the UK Standard Contractual Clauses Addendum.