INKY HOSTED SERVICES AGREEMENT

This Inky Hosted Services Agreement ("Agreement") is entered into between **Inky Technology Corporation** with address at 1452 Hughes Rd Ste 200 PMB 530, Grapevine, TX ("Inky"), and Customer. Inky and Customer are each a "Party" to this Agreement and are together referred to herein as the "Parties." The terms and conditions of this Agreement shall control in the event any conflicting or differing terms and conditions are contained in any related document, including the Quotation or similar form, even if signed by the Parties after the date hereof, unless expressly provided for in this Agreement. Each Party's acceptance of this Agreement is expressly conditional upon the other's acceptance of the terms contained in the Agreement to the exclusion of all other terms. For good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows. The foregoing text is incorporated herein by reference.

1. DEFINITIONS.

1.1 "Confidential Information" is as defined in Section 5.1 of this Agreement.

1.2 "Customer Data" means any data or information relating to Customer, generated by and/or through Customer's access to and/or use of the Platform, or which was acquired by Inky during the course of providing the Platform to Customer, including Customer Confidential Information, Personal Information, information on individual phishing attacks on Customer, Customer data, and email content (including associated meta-data).

1.3 "Dashboard Data" means meta-data retained by Inky for the purposes of providing an analysis tool to Customer and to populate Customer's administration console. The administration console allows Customer to view current and historical decisions made by the Platform, to assess current threats, and to intuit overall security/situational awareness.

1.4 "Disaster Recovery Plan" is as defined in Section 16 of this Agreement.

1.5 "End Users" means employees, contractors and/or other Customer agents or representatives having a Customer-issued email address that use the Platform.

1.6 "Hosting Provider" means the provider hosting the Platform as identified in the Data Processing Addendum and any successor thereto.

1.7 "Hosting Services" means the provision of on-demand online access to the Platform by the Hosting Provider in accordance with the terms of service referenced herein.

1.8 "Intellectual Property Rights" means any and all: (i) registered and unregistered rights granted, applied for or otherwise now or hereafter in existence under or related to any patent, copyright, trademark, trade secret, design, mask work, typography, database protection, or other intellectual property rights or proprietary rights laws, (ii) similar or equivalent rights or forms of protection arising under statutory or common law, contract, or otherwise, and whether or not perfected, (iii) goodwill associated with the foregoing, and (iv) customizations,

enhancements, improvements, modifications and derivative works of and to the foregoing described in (i) through (iv), as may now or in the future exist in any part of the world, in all media, for all versions and elements, in all languages, and for the entire duration of such rights.

1.9 "Inky Property" is as defined in Section 7 of this Agreement.

1.10 "Learned Data" is as defined in Section 6.4 of this Agreement.

1.11 "Personal Information" means any non-public personal information of a Party or its customers that is protected by any law applicable to such Party and is disclosed by a Party to the other Party in connection with this Agreement.

1.12 "Platform" means the hosted Inky anti-phishing security solution described in the Quotation.

1.13 "Quotation" means the initial subscription order attached hereto as Exhibit B, titled Product & Services Quotation, and any renewal subscription order(s).

1.14 "Term" is as defined in Section 4.1 of this Agreement.

2. LICENSE, SERVICES AND SUPPORT.

2.1 Subject to the terms and conditions of this Agreement, Inky will use a Hosting Provider to host the Platform and hereby grants Customer a revocable, non-transferable, and non-exclusive right to access and use the Platform remotely. Customer may only access and use: (a) the Platform for its intended purpose and in the ordinary course of its business; and (b) the services provided by the Hosting Provider in connection with this Agreement for its intended purpose as related to the Platform and in the ordinary course of its business.

2.2 Customer is solely responsible for completing any implementation and onboarding steps located at https://www.inky.com/hubfs/Exhibit_A_-_Inky_Onboarding.pdf, which are minimum requirements necessary to allow Inky to enable and activate the Platform for Customer, the terms, steps, and procedures, which are incorporated herein by reference.

2.3 Inky will exercise commercially reasonable efforts to provide the level and type of support for the Platform, during normal business hours and in accordance with its Support & Service Level Agreement, attached hereto as Exhibit C. Customer, at no extra charge, shall be entitled to receive any enhancements, modifications, fixes and/or improvements to the Platform that Inky generally makes in its routine support and maintenance of the Platform.

3. PAYMENT OF FEES.

3.1 Upon execution of this Agreement and its associated Quotation or the execution of subsequent Quotations for a Renewal Term (as hereinafter defined), Inky will invoice Customer the full amount indicated in the Quotation within ten (10) business days, unless indicated otherwise in the Quotation.

3.2 Customer will pay Inky the applicable Fees set forth in the Quotation (the "Fees"). The initial Quotation in connection with this Agreement is attached hereto as Exhibit B. If in any given month during the Term, Customer's use of the Platform exceeds any use limitations set forth in the Quotation, Customer will be invoiced at the end of each calendar month for the excess usage at the per user rate set forth in the Quotation, and Customer agrees to pay the additional undisputed Fees without any right of set-off or deduction. All payments will be made in accordance with the payment terms set forth in this Section 3, unless otherwise set forth in the Quotation.

3.3 Customer will pay Inky Fees invoiced within thirty (30) days of receipt by Customer of an invoice. In the event Customer's account is more than thirty (30) days overdue on payment for any reason, Inky shall provide written notice to Customer of such condition and Customer shall have thirty (30) days from receipt of such notice to cure the overdue condition of its account. In the event Customer fails to cure the overdue condition of its account within thirty (30) days after receipt of such notice from Inky, then Inky shall have the right, in addition to its remedies under this Agreement or pursuant to applicable law, to immediately suspend access to or use of the Platform without further notice to Customer, until Customer has paid the balance owed in full.

3.4 In the event this Agreement is renewed, Fees may not be increased by more than ten (10%) percent of the Fees applicable in the immediately prior term.

3.5 Fees under this Agreement are exclusive of all taxes, including national, state or provincial and local use, sales, value-added, property and similar taxes, if any. Customer agrees to pay such taxes that are assessed and lawfully imposed on the Customer (and for which no exemption is available) (excluding taxes measured by or based on Inky's gross or net income, or gross or net receipts (including any capital gains or minimum taxes) or capital, doing business, excess profits, net worth, franchise, property, and Inky personnel-related taxes) unless Customer has provided Inky with a valid exemption certificate authorized by the appropriate tax authority. In the case of any withholding requirements, Customer will pay any required withholding itself and will not reduce the amount to be paid by Customer on account thereof.

4. TERMINATION.

4.1 Subject to early termination as provided in this Agreement, the subscription period for the Platform begins on the Start Date specified in the Quotation and ends on the End Date specified in the Quotation (such period, the "Initial Term"). After the Initial Term, the Agreement shall automatically renew for one (1) year renewal terms (each, a "Renewal Term") unless either Party gives prior written notice of its intent not to renew the Agreement at least thirty (30) days before the end of the then-current Term, as applicable. The Initial Term and any Renewal Terms are referred to collectively as the "Term."

4.2 In the event of any material breach of this Agreement, the non-breaching Party may terminate this Agreement prior to the end of the then-existing Term by giving thirty (30) days' prior written notice of said breach to the breaching Party; provided, however, that this Agreement will not terminate if the breaching Party has cured the breach prior to the expiration of such thirty (30) day period.

4.3 Either Party may terminate this Agreement, without notice, (i) upon the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings, (ii) upon the other Party's making an assignment for the benefit of creditors, or (iii) upon the other Party's dissolution or ceasing to do business or becoming insolvent, failing to pay, or admitting in writing its inability to pay debts as they become due.

4.4 Except for termination due to Customer's breach of this Agreement and/or any Quotation, upon any termination Inky will refund to Customer the unused pro rata portion of any prepaid Fees to the date of termination within thirty (30) days following termination.

4.5 Following termination and upon Customer's request, within fifteen (15) days following termination, Inky will provide to Customer, at no charge to Customer, any Customer Data then in its possession in an industry standard encrypted electronic format and will delete all copies of Customer Data then in its possession from its computer systems and use reasonable efforts to delete any references to Customer from its computer systems, Learned Data and Dashboard Data excepted; provided, however, that Inky may retain a copy of Customer Data it deems necessary to comply with its internal retention policies or any obligations under all applicable law and any Confidential Information it believes cannot reasonably be destroyed (such as oral communications reflecting Confidential Information, electronic mail back-up records, back-up server tapes and any similar such automated record-keeping or other retention systems), which shall remain in perpetuity subject to the Confidentiality (Section 5) provision of this Agreement.

4.6 Inky may immediately suspend, terminate or otherwise deny Customer, any of its End Users, or any other person's access to or use of all or any part of the Platform, without incurring any resulting obligation or liability, if: (a) Inky receives a judicial or other governmental demand or order, or law enforcement request that expressly or by reasonable implication requires Inky to do so; provided, however, that Inky shall notify Customer within ten (10) business days of this action to allow

Customer, at its expense, to defend against such governmental demand or order, or law enforcement request; or (b) Inky believes, in its good faith discretion, that: (i) Customer or any End User has failed to comply with, any term of this Agreement, or accessed or used the Platform beyond the scope of the rights granted or for a purpose not authorized under this Agreement; (ii) Customer or any End User is or has been involved in any fraudulent or unlawful activities relating to or in connection with any use of the Platform; or (iii) this Agreement expires or is terminated. This Section 4.6 does not limit any of Inky's other rights or remedies, whether at law, in equity or under this Agreement.

4.7 Upon any termination or expiration of this Agreement, Customer shall promptly pay all amounts due and remaining payable through the date of such termination or expiration hereunder. Furthermore, upon expiration or termination of this Agreement, Customer will, and will ensure that all End Users will, immediately cease all use of the Platform and delete all copies of Inky Property in its control, and all rights licenses, consents and authorizations granted by Inky to Customer hereunder will immediately terminate. Upon Inky's request, Customer will confirm in writing that it has complied with the terms of this provision.

4.8 All sections of this Agreement which by their nature should survive termination will survive termination, including, without limitation, restrictions, accrued rights to payment, confidentiality obligations, intellectual property rights, warranty disclaimers, and limitations of liability.

5. CONFIDENTIALITY.

5.1 Each Party (the "Receiving Party") understands that the other Party (the "Disclosing Party") has disclosed or may disclose non-public or proprietary information including but not limited to information relating to the Disclosing Party's technology or business identified as proprietary or confidential, or which given its nature and the circumstances surrounding its disclosure should reasonably be construed to be confidential including, without limitation Customer Data and Personal Information (hereinafter referred to as "Confidential Information" of the Disclosing Party). The Receiving Party agrees: (i) not to disclose, divulge or otherwise make available to any third party any such Confidential Information, (ii) to give access to such Confidential Information solely to those employees or independent contractors with a need to have access thereto for purposes of this Agreement and who agree to policies and obligations consistent with the terms of this Agreement with respect to such Confidential Information or by the nature of the capacity in which they render services, it is implicit they assume obligations consistent with the terms of this Agreement and for which it shall be liable for the acts or omissions of such employees or independent contractors, (iii) to hold the other Party's Confidential Information in confidence and protect such Confidential Information from unauthorized disclosure and take the same security precautions to protect against disclosure or unauthorized use of such Confidential Information that the Party takes with its own proprietary information, but in no event will a Party apply less than commercially reasonable precautions to protect such Confidential Information, and (iv) not to use or duplicate the Confidential

Information of the other Party for any purpose other than to perform its obligations or exercise its rights hereunder. The Disclosing Party agrees that the foregoing will not apply with respect to any information that the Receiving Party can document (a) is or becomes generally available to the public without any action by, or involvement of, the Receiving Party, or (b) was in Receiving Party's possession or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to Receiving Party without any obligations of confidentiality by a third party, or (d) was independently developed by or for Receiving Party without use of any Confidential Information of the Disclosing Party. Nothing in this Agreement will prevent the Receiving Party from disclosing the Confidential Information pursuant to any judicial or governmental order or request, provided that the Receiving Party gives the Disclosing Party reasonable prior notice of such disclosure (to the extent permitted by applicable law) to allow Disclosing Party to contest such order and the Receiving Party shall reasonably cooperate, at the Disclosing Party's expense, with the Disclosing Party in protecting against any such disclosure and/or obtaining a restraining or similar protective order. In the event that the parties are not successful in obtaining a protective order and the Receiving Party is, in the opinion of its counsel, compelled to disclose the Confidential Information, the Receiving Party may disclose such information solely in accordance with and for the limited purpose of compliance with the court order or governmental or regulatory requirement or request without liability hereunder and in any such event, the Receiving Party will use its reasonable best efforts (and will reasonably cooperate with the Disclosing Party in its efforts) at Disclosing Party's expense to ensure that such Confidential Information and other information that is so disclosed will be accorded confidential treatment.

5.2 Either Party has the right to disclose the existence but not the terms and conditions of this Agreement, unless such disclosure is approved in writing by both Parties prior to such disclosure, or is included in a filing required to be made by a Party with a governmental authority (provided such Party will use reasonable efforts to obtain confidential treatment or a protective order) or is made on a confidential basis as reasonably necessary to potential investors or acquirers.

5.3 Upon written request at any time, the Receiving Party will return to the Disclosing Party in an industry standard encrypted electronic format, or destroy at the Disclosing Party's request, any and all of the Disclosing Party's Confidential Information then in the Receiving Party's possession or control and, if destroyed, provide the Disclosing Party with written confirmation of such destruction, provided that the Receiving Party may retain one (1) encrypted copy of the Confidential Information it deems necessary to comply with its internal retention policies or any obligations under all applicable law and any Confidential Information it believes cannot reasonably be destroyed (such as oral communications reflecting Confidential Information, electronic mail back-up records, back-up server tapes and any similar such automated record-keeping or other retention systems), which shall remain subject to the confidentiality terms of this Agreement in perpetuity.

6. INTELLECTUAL PROPERTY RIGHTS.

6.1 Except as expressly set forth herein, as between Inky and Customer, Inky alone (and its licensors, where applicable) will retain all Intellectual Property Rights relating to (i) Inky Property, the Platform, including without limitation, improvements, enhancements, additions or other modifications made thereto, or (ii) any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Customer or any third party relating to the Inky Property, the Platform, which are hereby assigned to Inky. Customer will not copy, distribute, reproduce or use any Inky Property except as expressly permitted under this Agreement.

6.2 Subject to Customer's payment of applicable Fees and compliance with the terms and conditions of the Agreement, Inky hereby grants Customer a limited, non-exclusive, revocable (as provided herein), non-sublicensable, royalty-free right and license during the Term to use solely that portion of the Inky Property generated or provided by the Platform specifically for Customer in the administration console pursuant to this Agreement, solely internally, and in the ordinary course of its business, including any documentation, reports, analyses, in each case, each made part of such Inky Property. Other than the right to access and use the Platform, and the limited non-exclusive license to use Inky Property during the Term of this Agreement, nothing in this Agreement shall be construed to, or be deemed to, assign or grant to Customer any right, title, or interest in or to the Platform or Inky Property relating thereto.

6.3 By using the Platform, Customer acknowledges and agrees for Inky to obtain, collect, and process Customer Data for the performance of its obligations under this Agreement. Such processing may include, but is not limited to, reading, scanning, analyzing Customer Data, and modifying Customer Data through functionalities of the Platform. Modifications may also include authorized End Users authorizing Inky through the Platform to delete Customer Data, such as emails. Subject to the terms of this Agreement, Customer is and will remain the sole and exclusive owner of all right, title, and interest in and to all Customer Data.

6.4 Customer hereby grants to Inky and its respective officers, directors, members, managers employees, subcontractors, and agents an irrevocable, royalty-free, worldwide right and license to access, collect, analyze, and use Customer Data collected and/or received by Inky: (i) during the Term, solely as necessary to provide the services associated with the Platform to Customer and its End Users; (ii) in perpetuity, to the extent Inky is using Customer Data by aggregating it with similar data of other Inky customers and de-identifying and anonymizing it so it does not identify Customer as the source of Customer Data or any part thereof, to improve and enhance its products and services ("Learned Data"), provided that the Learned Data does not include any Customer Confidential Information; and (iii) to display, among other things, Dashboard Data in the administration console of the Platform to authorized End Users.

7. RESTRICTIONS AND RESPONSIBILITIES.

Customer will not, and will not permit anyone else, to: (i) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, algorithms or models of the Platform, its software, and the data generated or provided by the Platform (collectively, "Inky Property") (provided that reverse engineering is prohibited only to the extent such prohibition is not contrary to applicable law); (ii) modify, translate, or create derivative works based on Inky Property; (iii) use Inky Property for any purpose other than its own internal use for the benefit of its End Users; (iv) use Inky Property for the development, provision or use of a competing software service or product; or (v) use Inky Property other than in accordance with this Agreement and in compliance with all applicable laws and regulations.

8. INDEMNIFICATION.

8.1 Indemnification by Inky.

(a) Inky shall defend, indemnify and hold harmless Customer and its respective officers, directors, employees, and agents (together with the Customer, collectively "Customer Indemnified Persons") from any finally adjudicated third party claims, liabilities, counterclaims, suits, demands, actions, damages, (including, but not limited to, any judgement, arbitration award or court approved settlement and reasonable attorneys' fees) or allegations arising out of any claim by a third party (i) that the Platform or any materials provided by Inky to Customer, infringe any patent or copyright, or misappropriate any trade secret, of such third party, (ii) arising from the gross negligence, willful misconduct or fraudulent actions of Inky and/or its employees, directors, managers, members, officers or agents in the performance of their obligations under this Agreement, or (iii) based upon any failure by Inky or its employees, directors, officers or agents to comply with applicable law and regulations in the performance of their obligations under this Agreement; provided, however, Inky is promptly notified of the adjudicated result of any and all such claims. Customer further agrees to notify Inky upon the knowledge or discovery of the initiation of any and all such claims covered by this Section 8.1. Upon notification, Inky may, within fifteen (15) days of notification, elect to control and defend Customer against such claims; provided, however, that Inky shall obtain the express prior written approval of the Customer Indemnified Persons for any settlement that requires any specific performance or non-pecuniary remedy by the Customer Indemnified Persons, requires the payment of any amount by the Customer Indemnified Persons or does not provide an unconditional release to the Customer Indemnified Persons, further provided Inky is given sole control over the defense and/or settlement discussions thereof, and all reasonably requested assistance (at Inky's expense) in connection therewith. If Inky elects to defend Customer in such claim, Customer may retain its own counsel, at its own expense, subject to Inky's rights herein. The foregoing obligations set forth in this Section 8.1 do not apply with respect to portions or components of the Platform to the extent such services are (u) not created by Inky, (v) result in whole or in part from Customer specifications, (w) are modified after delivery by Inky (other than modifications made by or on behalf of Inky), (x) combined with other

products, processes or materials where the alleged infringement relates to such combination unless such combination was installed or implemented at the direction of Inky, (y) where Customer continues the allegedly infringing activity after being notified thereof or after being informed of modifications that would have avoided the alleged infringement, or (z) where Customer's use of the Platform is not strictly in accordance with this Agreement and all related documentation.

(b) If, due to a claim of infringement, the Platform is held by a court of competent jurisdiction to be or are believed by Inky to be infringing, Inky may, at its option and expense and in addition to its foregoing indemnification obligations (a) replace or modify the Platform to be non-infringing, provided that such modification or replacement contains substantially similar features and functionality, (b) obtain for Customer the appropriate license to allow Customer to continue using the Platform, or (c) terminate this Agreement. In the event of termination, Inky will refund Customer any unused pro rata portion of prepaid Fees. The foregoing states the entire liability of Inky with respect to the foregoing grounds for indemnification

8.2 Indemnification by Customer. Customer shall defend, indemnify and hold harmless Inky and its respective officers, directors, members, managers employees, and agents (together with Inky, collectively "Inky Indemnified Persons") from any third party claims, liabilities, counterclaims, suits, demands, actions, damages, (including, but not limited to, any judgement, arbitration award or court approved settlement and reasonable attorneys' fees) or allegations arising out of any claim by a third party (i) that Customer Data, when used in accordance with this Agreement, infringe or misappropriate any Intellectual Property Rights of such third party, or (ii) arising from the gross negligence (including breach of confidentiality obligations), willful misconduct or fraud of Customer and/or its employees, directors, officers or agents in the performance of their duties under this Agreement, or (iii) based upon any finally adjudicated failure by Customer or its employees, directors, officers or agents to comply with applicable law and regulations in the performance of their obligations under this Agreement; provided, however, that Customer shall obtain the express prior written approval of Inky Indemnified Persons for any settlement that requires any specific performance or non-pecuniary remedy by Inky Indemnified Persons, requires the payment of any amount by Inky Indemnified Persons or does not provide an unconditional release to Inky Indemnified Persons, further provided that Customer is promptly notified of any and all such claims, and given sole control over the defense and/or settlement thereof, and all reasonably requested assistance (at Customer's expense) in connection therewith. Inky may retain its own counsel, at its own expense, subject to Customer's rights herein.

9. WARRANTIES AND WARRANTY DISCLAIMER.

9.1 Each Party represents and warrants that it has all right, power and authority to enter into this Agreement and to grant the rights granted by it under this Agreement.

9.2 EXCEPT AS PROVIDED IN THIS AGREEMENT AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PLATFORM AND THE ASSOCIATED SERVICES AND SOFTWARE SUPPORTING THE PLATFORM, AND ALL RELATED INFORMATION (INCLUDING THE CONFIDENTIAL INFORMATION OF INKY), TECHNOLOGY AND SERVICES PROVIDED BY OR ON BEHALF OF INKY ARE PROVIDED "AS IS" AND "WHERE IS" AND WITHOUT ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AND INKY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (EVEN IF INKY IS ADVISED OF THE PURPOSE), TITLE, NON-INFRINGEMENT, OR ACCURACY. IN ADDITION, INKY DOES NOT WARRANT THAT THE PLATFORM AND THE ASSOCIATED SERVICES AND SOFTWARE SUPPORTING THE PLATFORM WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT THEY WILL MEET CUSTOMER'S NEEDS, OR THAT ANY DATA WILL NOT BE LOST.

9.3 Without limiting any of the foregoing and in addition thereto, no guarantee is made that the Platform eliminates any or all risk of loss, damage, or unauthorized access to Customer's information systems, software and equipment, or other unwanted effects on Customer's infrastructure or business, including the inability or the excessive delay to send or receive emails, as the result of processing emails for email-based threats (whether or not detected by the Platform), and Inky assumes no obligation or liability with respect to any of the foregoing. It is not possible to detect or alert End Users to all threats, and there is no guarantee that End Users will observe and take appropriate action with respect to any alerts the Platform provides. Inky is not responsible for any failure by any End User to observe or comprehend any alert issued by the Platform, or for any action or inaction taken by End Users in response to any such alerts. The Platform is intended to be part of, and not a substitute for, Customer's implementation of sound information security practices.

9.4 Inky represents and warrants that (i) it will provide the Platform in a professional and workmanlike manner consistent with then-existing industry standards and practices and will minimize errors and disruptions during the Term of this Agreement, (ii) for a period of ninety (90) days from the Effective Date of this Agreement, the Platform shall conform in all material respects to any documentation or specifications provided by Inky to Customer, (iii) for a period of ninety (90) days from the Effective Date of this Agreement, the functionality of the Platform will not be materially decreased during the Term, (iv) the Platform's source code will not intentionally contain any harmful computer code, viruses, worms, time-bombs, disabling features, tracking devices, trap doors, or code that will enable access to the Customer's systems code, files, scripts, agents or programs intended to do harm, including without limitation Trojan horses, malware, vulnerabilities, advanced persistent threats, exploits, code injections and targeted attacks, (v) it owns all rights, title, and interest in and to, the Platform and materials claimed to be its intellectual property which do not and will not violate the Intellectual Property Rights, or any other rights of any person or infringe or misappropriate any third party's rights, and (vi) it will comply with all applicable

laws, regulations, and ordinances applicable to its performance under this Agreement.

10. LIMITATION OF LIABILITY.

NEITHER PARTY WILL BE LIABLE FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN ANY WAY CONNECTED WITH THE USE OF THE PLATFORM OR ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT OR THE PLATFORM, THE DELAY OR INABILITY TO USE THE PLATFORM OR OTHERWISE ARISING FROM THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, LOSS OF REVENUE OR ANTICIPATED PROFITS OR LOST BUSINESS OR LOST SALES, WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR OTHERWISE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. THE TOTAL LIABILITY OF EITHER PARTY, WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), OR OTHERWISE, WILL NOT EXCEED, IN THE AGGREGATE, AN AMOUNT EQUAL TO THE FEES PAYABLE TO INKY HEREUNDER IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRIOR TO THE EVENT GIVING RISE TO THE CLAIM (OR IF SUCH EVENT OCCURS IN THE FIRST TWELVE (12) MONTHS OF THE AGREEMENT TERM, THE AMOUNT ESTIMATED TO BE PAID IN THE FIRST TWELVE (12) MONTHS OF THE TERM). THE FOREGOING LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

11. U.S. GOVERNMENT MATTERS.

Notwithstanding anything else, Customer may not provide to any person or export or re-export or allow the export or re-export of the Platform or any software or anything related thereto or any direct product thereof (collectively "Controlled Subject Matter") in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority. Without limiting the foregoing, the parties acknowledge and agree that the Controlled Subject Matter will not be used or transferred or otherwise exported or re-exported to countries as to which the United States maintains an embargo (collectively, "Embargoed Countries"), or to or by a national or resident thereof, or any person or entity on the U.S. Department of Treasury's List of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders (collectively, "Designated Nationals"). The lists of Embargoed Countries and Designated Nationals are subject to change without notice. Use of the Platform is a representation and warranty by the Customer that it and its End Users are not located in, under the control of, or a national or resident of an Embargoed Country or Designated National. The Controlled Subject Matter may use or include encryption technology that is subject to licensing requirements under the U.S. Export Administration Regulations. As defined in FAR section 2.101, the Platform, any software and documentation provided by Inky are "commercial items" and according to DFAR section 252.227-7014(a)(1) and (5) are deemed to be "commercial computer software" and "commercial computer software documentation." Consistent with DFAR section 227.7202 and FAR section 12.212, any use modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software

documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

12. HOSTING PROVIDER.

12.1 Hosting Provider. Customer acknowledges and agrees that the Hosting Services are provided by and made available to the Customer by a hosting provider identified in the Data Processing Addendum (Exhibit D) (the "**Hosting Provider**"), which is authorized to make modifications and enhancements to the Hosting Services at any time and in its discretion. The term Hosting Provider shall include any and all successors thereto. Customer's ability to use the Platform is dependent upon the availability and capabilities of the Hosting Services and may be affected or limited by the Hosting Services. CUSTOMER IS AT ALL TIMES IS RESPONSIBLE FOR ADHERING TO THE ENCRYPTION METHODS PROVIDED BY INKY AND HOSTING PROVIDER WHILE CUSTOMER DATA IS IN TRANSIT TO AND FROM THE HOSTING PROVIDER OR WHEN PROCESSED OR STORED BY HOSTING PROVIDER.

12.2 Hosting Provider & Hosting Services. Customer acknowledges and agrees that Inky will not be liable for any interruption, unavailability or outage to the Hosting Services or the Platform, and any interruption, unavailability or outage of the Customer's systems, or unauthorized access to or use of Customer Data caused by any such third-party Hosting Provider that is not within Inky's reasonable control.

13. DATA PROTECTION AND INFORMATION SECURITY.

13.1 Inky will implement and maintain a comprehensive written information security program that includes appropriate administrative, technical, and physical safeguards and other security measures designed to: (A) ensure the security and confidentiality of such Customer Data; (B) protect against any anticipated or reasonably likely threats or hazards to the security or integrity of such Customer Data; (C) protect against any actual or suspected unauthorized access to or use, disclosure, processing or acquisition of such Customer Data (hereinafter, an "Information Security Incident"); and (D) ensure the proper disposal of Customer Data. Inky shall promptly notify Customer in writing within 72 hours of its confirmation of the occurrence of an Information Security Incident of which Inky becomes aware. Such notice shall summarize in reasonable detail the effect on Customer, if known, of the Information Security Incident and the corrective action taken or to be taken by Inky. Inky shall within seven (7) days take all necessary and advisable corrective actions, and Customer shall cooperate fully with Inky in all reasonable and lawful efforts to prevent, mitigate or rectify such Information Security Incident. Inky shall (i) investigate such Information Security Incident; and (ii) to the extent reasonably practical, remediate the effects of such Information Security Incident. If Inky issues any press releases or reports or makes any public filings related to any Information Security Incident, then it will make a copy available to Customer. Inky will reasonably assist Customer with any and all reporting, audit, and/or notification obligations incurred by Customer relating to an Information Security Incident. If to the extent that the Information Security Incident was caused by Inky's material breach of this Section 13.1, Inky shall

reimburse Customer for costs incurred by Customer relating to with remediation, reporting, and notification of such incident, net of any insurance proceeds actually recovered by Customer.

13.2 To the extent that Customer Data is subject to the California Consumer Privacy Act ("CCPA") or the General Data Protection Regulation ("GDPR") of the European Union, the Data Processing Addendum, attached as Exhibit D, shall apply to such Customer Data, and is hereby incorporated into this Agreement by reference. Customer is solely responsible for determining whether Customer Data is subject to CCPA and GDPR.

14. ACCESS.

14.1 Access Controls. Unauthorized Access. Inky will exercise commercially reasonable efforts to prevent unauthorized access to the computer systems, and any databases or files containing Customer Data. Inky will exercise commercially reasonable efforts to prevent unauthorized destruction, alteration or loss of Customer's information contained in its computer systems. Inky will maintain an audit log of access to the Platform, which it will provide to Customer promptly upon request. To maintain the integrity of its computer systems, Inky will install all security upgrades and patches with respect to its computer systems as soon as reasonably possible. If Inky is to be provided with access to Customer's computer systems, in connection with this Agreement, Inky and its personnel will be required to execute a separate system access agreement before such access is granted, which agreement will be deemed a part of this Agreement.

14.2 Access List. At Customer's request, Inky will provide Customer with a list of all End Users that are authorized to access Customer's administration console.

14.3 Customer Access Control. Customer is responsible for establishing unique account credentials for any users who will have access to any administrative functions of the Platform, and for removing account credentials for any administrative users if Customer wishes to suspend or terminate their access to administrative functions. Customer will be solely responsible for all activity occurring under user accounts established by or for Customer.

15. INSURANCE.

During the Term of this Agreement, Inky will maintain the insurance coverages outlined in Exhibit A, attached hereto.

16. DISASTER RECOVERY PLAN.

If the Platform is interrupted for any reason other than scheduled maintenance, Inky will activate its disaster recovery plan, which is located at https://www.inky.com/hubfs/Exhibit D-Disaster Recovery Plan.pdf ("Disaster Recovery Plan"), so that the Platform will continue without further interruption and will notify Customer of this activation. Inky will keep the Disaster Recovery Plan in effect during the term; provided, however, that Inky reserves the right to adjust the Disaster Recovery Plan on an as-needed business basis without notice to Customer, but in no event shall Inky significantly decrease the quality of the Disaster Recovery Plan. During the Term, Inky will test its disaster recovery plan not less often than annually and will promptly deliver the results of each test to Customer upon request.

17. MISCELLANEOUS.

17.1 Survival. If any provision of this Agreement is found to be unenforceable or invalid, that provision will be eliminated or limited to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

17.2 Entire Agreement. Both parties acknowledge and agree that this Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both parties, except as otherwise provided herein.

17.3 Relationship of Parties. No agency, partnership, joint venture, or employment is created as a result of this Agreement and neither Party has any authority of any kind to bind the other Party in any respect whatsoever.

17.4 Subcontractors. Inky is authorized to use subcontractors in the performance of its obligations under this Agreement; provided that said subcontractors are not from any countries sanctioned by the Office of Foreign Assets Control (U.S. Department of the Treasury) and that they do not have access to Customer Data.

17.5 Reserved.

17.6 Governing Law and Venue. This Agreement will be governed by the laws of the State of Maryland, U.S.A. without regard to its conflict of laws provisions. The federal and state courts located in or having jurisdiction over Montgomery County, Maryland will have proper and exclusive jurisdiction and venue with respect to any disputes arising from or related to the subject matter of this Agreement. NEITHER PARTY NOR ITS COUNSEL SHALL ELECT A TRIAL BY JURY IN ANY ACTION, SUIT, PROCEEDING OR COUNTERCLAIM ARISING OUT OF OR IN ANY WAY CONNECTED WITH THIS AGREEMENT.

17.7 Attorneys' Fees. In any action or proceeding brought to enforce any provision of this Agreement, including the collection of Fees, Inky shall, to the extent permitted by applicable law, be entitled to reasonable attorney's fees, costs, ad and expenses.

17.8 Force Majeure. Neither Party shall be liable under this Agreement for failure or delay in the performance of its obligations (except for payment of Fees) for reasons of strikes, shortages, riots, insurrection, fires, floods, storms, explosions, acts of God, war, governmental actions, labor conditions, earthquakes, material shortages, failures of internet service providers, utilities, and/or telecommunication providers, or any other cause which is beyond the reasonable control of such Party.

17.9 Assignment. Customer may not assign or transfer this Agreement in whole or in part by operation of law or otherwise, without Inky's prior written consent which consent shall not be unreasonably withheld or delayed. Any attempt by Customer to transfer or assign this Agreement without such written consent will be null and void and may be deemed by Inky to be a material breach of this Agreement. Notwithstanding the foregoing, either Party may assign this Agreement without consent of the other Party to the acquiring or surviving entity in a merger or acquisition in which either Party is the acquired entity (whether by merger, reorganization, acquisition or sale of stock) or to the purchaser of all or substantially all of either Party's assets and shall provide prompt notice of such assignment to the other Party. This Agreement will be binding upon the parties and their respective legal successors and permitted assigns.

17.10 Reserved

17.11 Publicity. Inky may use Customer's name for advertising, trade or other commercial purposes without Customer's express prior written consent. Inky and its contractors, employees and agents shall not hold themselves out as an employee, affiliate, or subsidiary of Customer at any time while performing services under this Agreement. Any materials provided to Inky by Customer pursuant to this Agreement or in connection with Inky's performance of services hereunder, bearing any Customer names, logos, styles or trademarks may be used by Inky only as necessary to perform services under this Agreement.

17.12 Third Party Beneficiaries. This Agreement has been entered into for the sole benefit of the parties and their respective permitted successors and assigns. Except as specifically set forth in this Agreement, the parties do not intend the benefits of this Agreement to inure to any third party, and nothing contained herein shall be construed as creating any right, claim or cause of action in favor of any such third party against any party.

Included Exhibits:

Exhibit A: Insurance
Exhibit B: Quotation
Exhibit C: Inky Support & Service Level Agreement
Exhibit D: Inky's Disaster Recovery Plan
Exhibit E: Inky's Data Processing Addendum (DPA)

EXHIBIT A

INSURANCE

During the Term of this Agreement, Inky shall maintain insurance in the minimum amounts as follows:

(i) Worker's Compensation Insurance: Statutory Workers Compensation in accordance with all state and local requirements of the state(s) in which Inky has a business office;

(ii) Employers Liability insurance with minimum occurrence limits as follows:

- Bodily injury by accident $100,000 each accident,
- Bodily injury by disease $500,000 policy limit, and
- Bodily injury by disease $100,000 each employee;

(iii) Commercial General Liability Insurance, written on an occurrence basis, including bodily injury, property damage, personal injury, advertising injury, products and completed operations, and contractual liability, in an amount not less than:

- Products/Completed Operations Aggregate Limit $1,000,000,
- Advertising Injury and Personal Injury Limit $1,000,000, and
- General Aggregate $2,000,000;

(iv) Property Insurance:

- Covering the replacement value of any and all property of Customer which may be in Inky's care, custody and/or control during the term of this Agreement up to $5,000;
- Covering the replacement value of any and all property of Customer that may be used on Customer premises in connection this Agreement, up to $10,000;

(v) Cyberinsurance in the amount of $5,000,000 covering loss, damage, liability, cost or expense arising from, or in any way attributable to, an "Information Security Incident" involving Personal Information in Inky's possession, custody or control, or for which Inky is otherwise responsible. The Cyberinsurance Inky will maintain for the purposes of this Section (v) shall include, without limitation, coverage for legal fees; notifications; investigation/forensic and restoration costs; crisis management/public relations; credit monitoring/identity protection services; call center expenses; and extra expense/business interruption.

(vi) All insurance policies provided and maintained by Inky shall be underwritten by insurers that are rated "A-VII" or higher.

Certificates of Insurance and evidence of the foregoing endorsements shall be provided to Customer upon request. Such Certificates shall provide that the insurer will give thirty (30) days' written notice to Customer prior to cancellation of any policy or endorsement or any change in policy coverage or coverage amounts.

EXHIBIT C

INKY SLA

1. **Definitions**. For purposes of this SLA the following definitions will apply.
    i. "Scheduled Maintenance Window" means the window during which weekly scheduled maintenance of the Product may be performed. The Scheduled Maintenance Window shall be provided to the Customer in writing in advance of any scheduled maintenance.

    ii. "Emergency Maintenance" means any time outside of Scheduled Maintenance Window that Inky is required to apply urgent patches or fixes, or undertake other urgent maintenance activities. If Emergency Maintenance is required, Inky will provide the expected start time and the planned duration of the Emergency Maintenance and if Inky expects the Product to be unavailable during the Emergency Maintenance through the Inky support site.

    iii. "System Availability" means the percentage of total time during which the Product is available to Customer, excluding Scheduled Maintenance Window and Emergency Maintenance.

2. **Service Credits**
    i. For each of the SLAs in this Exhibit C, if in any calendar month the SLA is not met and if the Customer has fulfilled all of its obligations under the Agreement and the SLA, The Customer will be provided with a Service Credit for the month in which the failure to meet the SLA has occurred. The Service Credit will be calculated in accordance with the tables in Section 6 of this SLA. Notwithstanding any to the contrary in this Agreement, such Service Credit is the sole remedy for the Customer and sole liability for Inky for Inky's failure to meet any obligation under this SLA.

    ii. "Service Credit" means the percentage of the monthly fees paid or payable for Product that is awarded to the Customer for a validated claim associated with the Service related to breach of the applicable SLA during that month.

    iii. In any given month, the Customer shall in no event be entitled to receive a credit that exceeds 100% of its monthly fee for the Product.

    iv. Any Service Credits earned by the Customer hereunder will be applied to the fees owed by the Customer for the next invoice for which the Service Credit applies. Service Credits earned by the Customer hereunder will be applied against amounts due for the next invoice. If Service Credits cannot be applied to future fees because the Agreement has terminated due to Inky's breach of the Agreement, the Customer will be paid the amount of the Service Credit immediately upon termination.

3. **SLA Claims**
    i. It is the parties' intention that all SLA claims be machine-verifiable. Specifically, Inky shall run scripts or similar automated tools to actively measure System Availability and other Service performance criteria in real time

    ii. All SLA claims must be made to Inky by the Customer. For the avoidance of doubt, SLA claims must reference the relevant machine-verifiable metric, as defined in Section 3(i).

    iii. Inky shall make information used to validate an SLA claim available for auditing by the Customer, at the Customers request.

    iv. In the event that more than one aspect of the Product is affected by the same root cause, the single SLA applicable to such Product of Customer's choosing may be claimed and no other claim will be validated or otherwise allowed for that event.

4. **SLA Overview**
    i. System Availability SLA
        a. Inky warrants at least 99.9% System Availability for the processing and delivery of email during each calendar month, excluding Scheduled Maintenance Window and Emergency Maintenance.

ii. Quarantine Mechanism

a. The Customer acknowledges that Inky does not operate an independent quarantine facility, but instead adds a set of headers to emails that should be quarantined. Physical quarantine shall be handled by the back-end email

iii. Email Delivery SLA

a. Inky warrants that the average of Email Delivery (as defined below) times, as measured in minutes over a calendar month, will be one (1) minute or less.

b. Customer shall not have any remedies under this SLA to the extent any SLA claim hereunder is due to (i) delivery of email to quarantine; (ii) email in deferral queues; or (iii) email loops.

c. Email delivery time shall be measured from the presentation of a message for processing by Inky to the handoff the message to the messages designated next hop.

5. SLA Schedules

System Availability	Service Credit
<99.9%	25%
<98.0%	50%
<97.0%	100%

Email Delivery	Service Credit
>1 minute	25%
>5 minutes	50%
>10 minutes	100%

6. Inky Support

i. INKY provides 24x7 support for emergency related outages and events via email at outage@inky.com. Emergency Issues are defined as those resulting in a service outage due to INKY hosted services not delivering email. In the event you report an emergency event INKY Engineers will begin investigation of the event within 30 minutes.

ii. For all non-emergency issues, INKY provides e-mail support during INKY's normal business hours of 9AM – 5PM Eastern Time. For non-emergency related issues, INKY can be reached at support@inky.com. Emails received during normal business hours will receive an initial response within one business day. All emails received outside of INKY's core business hours will receive an initial response the following business day.

INKY

Disaster Recovery Plan

Exhibit D

INKY Services

INKY Services are hosted on AWS infrastructure.

- INKY Phish Fence
- INKY Encryption
- INKY Analytics / Reporting / Configuration
- INKY Link Analysis

High Risk Services (Less than three region redundancy.)

INKY's database is a single master multi read replica configuration. Read Replicas are hosted in each active INKY AWS region. The master is hosted in AWS Region US-East-1 in a multi-availability zone deployment.

INKY has identified this as the largest design single point of failure in the current architecture design. Future plans will look to incorporate a MultiMaster design and currently the bulk of recovery planning centers on mitigations of this component.

INKY is able to be removed from mail flow by the client in the event of a significant outage allowing customers to restoremailflow.

Scenario: Region hosting the INKY database write master becomes unavailable.

RTO - 3 hours
RPO - < 30 minutes (Replication Lag time should be = to average replication lag)

AFFECT TO SERVICES:

INKYPhishFence – UNAFFECTED

- Mail Processing does not require write access to the INKY database.

INKYEncryption – UNAFFECTED

- The INKY Encryption service does not access the INKY database

INKY Analytics / Reporting / Configuration – DEGRADED / DEGRADED / DISRUPTED

- INKY dashboard services will be unable to incorporate new results until a write master database is available.

- Mail reported to the INKY service will not be reflected in results or analytics until a write master database is available.
- Configuration changes are not possible while the write master database is unavailable.

RECOVERY OUTLINE

- Identify unaffected region for new write master
- Create Snapshot of a current read replica in that region
- Launch that snapshot as a new write master database
- Update DNS to point to the new write master database
- Ensure that replication has resumed on read replicas

Scenario: Failure of a region hosting non-master database

RTO - 0
RPO - 0

AFFECT TO SERVICES:

INKYPhishFence – UNAFFECTED

- Mail Processing does not require write access to the INKY database.

INKYEncryption – UNAFFECTED

- The INKY Encryption service does not access the INKY database

INKY Analytics / Reporting / Configuration – UNAFFECTED

- INKY Analytics servers will be available in remaining regions
- Reporting services will be available in remaining regions
- Configuration services will be available in remaining regions

RECOVERY OUTLINE

- If outage is expected to be under 24 hours INKY operations will ensure all remaining regions have sufficient capacity.
- If outage is expected to exceed 24 hours a new available AWS region will be provisioned.
    - INKY utilizes Amazon Machine Images for all production systems. As a result, it is a straightforward process to bring additional regions on-line in the event of catastrophic failure
    - This process while straightforward will take approximately 24 hours to complete as new services will need to be warmed up and new IPs registered.

Scenario: Failure of all regions hosting INKY services

RTO - *

RPO - *

AFFECT TO SERVICES:

INKYPhishFence – UNAVAILABLE

- All Services down

INKYEncryption – UNAVAILABLE

- All Services down

INKY Analytics / Reporting / Configuration – UNAVAILABLE

- All Services down
- All Services down
- All Services down

RECOVERY OUTLINE

- INKY will provision a new AWS region as quickly as possible
    - INKY utilizes Amazon Machine Images for all production systems. As a result, it is a straightforward process to bring additional regions on-line in the event of catastrophic failure
- INKY Operations will identify if there is an alternate AWS region available to host INKY services.
- If no AWS region is available INKY services can be rebuilt onto alternate cloud services.
    - INKY Code / development and operations repositories are fully independent of AWS infrastructure.
    - INKY can rebuild all existing services on alternate cloud services platforms.

Exhibit E

INKY DATA PROCESSING ADDENDUM

Updated: April 8, 2022

THIS INKY DATA PROCESSING ADDENDUM (this "***DPA***") is hereby incorporated into the current version of the INKY HOSTED SERVICES AGREEMENT (the "***Agreement***") by and between Customer (as defined in the Agreement) and INKY TECHNOLOGY CORPORATION, a Delaware corporation ("***Inky***"), each a "***Party***" and collectively the "***Parties***."

This DPA applies to and takes precedence over the Agreement and any associated contractual document between the Parties, such as an order form or statement of work, to the extent of (but only to the extent of) any conflict or inconsistency between this DPA and the Agreement. Otherwise this DPA supplements and incorporates additional terms and conditions into the Agreement as and when it applies to the Platform provided under the Agreement.

1. **Definitions**. For purposes of this DPA, the following terms are defined and shall be interpreted as set forth below. Any capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement or (if not defined therein) applicable Data Protection Laws:

"***Affiliates***" means a company, person or entity that is owned or controlled by, that owns or controls or is under common ownership or control with a Party. Ownership shall mean direct or indirect ownership of more than 50% of the equity in a company or entity, and control shall mean any power to appoint persons to the board of directors of a company or entity or to operate and manage same.

"***Controller***" means (i) the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; or (ii) a "***Business***" as that term is defined in the CCPA.

"***Data Protection Laws***" means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, communications secrecy, breach notification, or the processing of Personal Data, including without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* ("***CCPA***") and the General Data Protection Regulation, Regulation (EU) 2016/679 ("***GDPR***"). For the avoidance of doubt, if Inky's processing activities involving Personal Data are not within the scope of a given Data Protection Law, such law is not applicable for purposes of this DPA.

"***Data Subject***" means an identified or identifiable natural person about whom Personal Data relates, including (i) an identified or identifiable natural person who is in the European Economic Area or whose rights are protected by the GDPR; or (ii) a "***Consumer***" as the term is defined in the CCPA.

"***Data Subject Rights***" means those rights identified in the GDPR and the CCPA granted to Data Subjects;

"***Personal Data***" includes "personal data," "personal information" and "personally identifiable information," and such terms shall have the same meaning as defined by the applicable Data Protection Laws.

"***Process***" and "***Processing***" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"***Processor***" means (i) a natural or legal person which processes personal data on behalf of the Controller; or (ii) a "***Service Provider***" as the term is defined in the CCPA.

"***Sale***" or "***Selling***" shall have the meaning defined in the CCPA.

"***Security Breach***" means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Personal Data.

"***Security Measures***" means description of the technical and organizational security measures implemented by Inky in its provision of the Platform to Customer as set out in Appendix 2 to Annex 1 of this DPA.

"***Sub-processor***" means (i) any processor engaged by the Processor or by any other Sub processor of the Processor who agrees to receive the Personal data exclusively intended for Processing activities to be carried out on behalf of the Controller after the transfer in accordance with Controller's instructions and in connection with the agreement for the provision of services to the Controller; or (ii) a Service Provider as defined in the CCPA;

"***Supervisory Authority***" means either (as applicable): (i) an independent public authority which is established by an EU Member State pursuant to Article 51 of the GDPR; or (ii) the California Attorney General.

2. **Scope and Purposes of Processing**.

(a) Inky will Process all Personal Data solely to fulfill its obligations to Customer under the Agreement and this DPA and on Customer's behalf, and for no other purposes, unless required to do otherwise by Data Protection Laws to which Inky is subject. In such case, Inky will inform Customer of that legal requirement before Processing, unless that law prohibits Customer from providing such information to Customer. With regard to the Processing of Personal Data, Inky will act as a Processor and Customer on which behalf the Personal Data is processed will act as Controller. Each Party will fully comply with the obligations that apply to it under the Data Protection Laws. The Personal Data shall remain at all times the Controller's property.

(b) Without limiting the foregoing, Customer directs Inky to Process Personal Data in accordance with Customer's written instructions, as may be provided by Customer to Inky from time to time and in the following manner.

(i) Subject matter, nature, and purpose of Processing: Inky will Process data solely to provide Customer with the Platform (including access to the Platform) (collectively, the "***Platform***") and to fulfill its purposes under the Agreement, which may include any lawful processing or business purposes as provided for under applicable Data Protection Laws. The Processing by Inky shall consist of all permitted processing operations under the Agreement necessary to provide the Platform.

(ii) Anticipated duration of Processing: For the term of the Agreement or to the extent that Inky continues to Process Personal Data (including for internal tax and audit purposes), whichever is longer.

(iii) Categories of Personal Data typically subject to Processing: All types of Personal Data including special categories of data, as that term is defined and permitted under applicable Data Protection Laws.

(iv) Typical categories of Data Subjects: All types of Data Subjects.

(c) Inky will immediately inform Customer if, in Inky's opinion, an instruction from Customer infringes Data Protection Laws.

(d) Inky will not:

(i) Sell Personal Data as defined in the CCPA.

(ii) Process Personal Data for any purpose other than for the specific purposes set forth herein. For the avoidance of doubt, Inky will not Process Personal Data outside of the direct business relationship between Customer and Inky or for a commercial purpose other than providing the Platform.

(iii) Attempt to link, identify or otherwise create a relationship between Personal Data and non-Personal Data or any other data except as authorized under the Agreement or as necessary to provide the Platform without the express authorization of Customer.

(e) For GDPR purposes, information that has been anonymized is not Personal Data. For CCPA purposes, information that has been de-identified is not Personal Data and Inky may de-identify Personal Data only if it:

(i) Has implemented technical safeguards that prohibit reidentification of the Data Subject to whom the information may pertain;

(ii) Has implemented business processes that specifically prohibit reidentification of the information;

(iii) Has implemented business processes to prevent inadvertent release of deidentified information; and

(iv) Makes no attempt to reidentify the information.

3. **Compliance with Data Protection Laws**.

(a) Inky will only Process Personal Data as set forth in this DPA and in compliance with Data Protection Laws.

(b) Inky hereby certifies that it understands its restrictions and obligations set forth in this DPA and will comply with them.

4. **Personal Data Processing Requirements**. Inky will:

(a) Ensure that the persons it authorizes to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(b) Upon written request of Customer, assist Customer in the fulfilment of Customer's obligations to respond to verifiable requests by Data Subjects (or their representatives) for exercising their Data Subject Rights (such as rights to access or delete Personal Data).

(c) Promptly notify Customer of (i) any third-party or Data Subject requests or complaints regarding the Processing of Personal Data; or (ii) any Supervisory Authority or Data Subject requests for access to or information about Inky's Processing of Personal Data on Customer's behalf, unless prohibited by Data Protection Laws. If Inky receives a third-party, Data Subject, or Supervisory Authority request, Inky will await written instructions from Customer on how, if at all, to assist in responding to the request. Inky will provide Customer with reasonable cooperation and assistance in relation to any such request.

(d) To the extent that Inky believes or becomes aware that its Processing or the Processing proposed by Customer of Personal Data is likely to result in a high risk (as defined in the applicable Data Protection Laws) with regard to the rights and freedoms of Data Subjects, it shall promptly inform the Customer and cooperate, at its own expense, as requested by the Customer to enable it to respond and comply with applicable Data Protection Laws, including providing reasonable assistance to and cooperation with Customer for Customer's performance of a data protection impact assessment of the Processing or proposed Processing of Personal Data.

(e) Provide reasonable assistance to and cooperation with Customer for Customer's consultation with any Supervisory Authority in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to Inky under Data Protection Laws to consult with a Supervisory Authority in relation to Inky's Processing or proposed Processing of Personal Data.

5. **Data Security**. Inky will implement appropriate administrative, technical, physical and organizational measures prior to and during Processing of any Personal Data to protect the security, confidentiality and integrity of the data and to protect the data against any form of Security Breach. Inky shall ensure a level of security appropriate to the risks presented by the processing of Personal Data and the nature of such Personal Data. Such measures shall include, as appropriate:

(a) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

(b) The ability to restore the availability and access to the Personal Data in timely manner in the event of a physical or technical security incident;

(c) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

At a minimum, such measures shall include the Security Measures which meet or exceed relevant industry practice. As of the Effective Date of the Agreement, Inky has implemented the Security Measures. Inky may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the material degradation of the security of the Platform.

6. **Duty to Notify and Cooperate**. Inky will promptly notify Customer and/or fully cooperate with Customer:

(a) If after a reasonable investigation, Inky becomes aware of any Security Breach relating to its or its Sub-processor's use or Processing of Personal Data. In such case, Inky shall promptly inform the Customer of the Security Breach without undue delay and shall provide all such timely information and cooperation as the Customer may reasonably require including in order for the Customer to fulfil its data breach reporting obligations under and in accordance with applicable Data Protection Laws. Inky shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Breach that are under its reasonable control and shall keep the Customer up-to-date about all developments in connection with the Security Breach. Inky shall also take all reasonable, necessary and appropriate steps to remedy any non-compliance with Data Protection Laws or cease further Processing of Personal Data, and the Controller may immediately terminate Inky's access to Personal Data or take any other necessary action as determined in its sole discretion;

(b) To enable the Customer to comply with its obligations with regard to the security of the Processing of Personal Data, taking into account the nature of the Processing and the information available to Inky;

(c) Upon the Customer's request, to make all such records, appropriate personnel, data processing facilities and any relevant materials available relating to the Processing of the Personal Data available to the Customer in order to allow the Customer to demonstrate compliance with its obligations laid down in applicable Data Protection Laws. In particular, the Customer or a third party appointed by the Customer (the "***Auditor***") may enter Inky's premises or the location where Personal Data is Processed, on reasonable notice during regular business hours and subject to appropriate confidentiality obligations, to verify Inky's compliance hereunder. The identity of the Auditor and the scope, timing and duration of the audit shall be separately agreed upon between the Parties. The Customer or the Auditor may also inspect, audit and review (but not remove sensitive network design or configuration data) any relevant records, processes and systems to verify compliance with the applicable Data Protection Laws and this DPA. The Customer shall take all reasonable measures to prevent unnecessary disruption to Inky's and/or its Sub-processor's operations. The audits will be at Customer's expense and Customer will not exercise its inspection rights as set forth in this clause more than once in any twelve (12) calendar month period and with at least thirty days' prior written notice, except (i) if and when required by instruction of a competent Supervisory Authority or (ii) the Customer believes a further audit is necessary due to a Security Breach by Inky.

7. **Subcontractors**.

(a) Customer acknowledges and agrees that Inky may use Inky affiliates and other subcontractors to Process Personal Data in accordance with the provisions within this DPA and Data Protection Laws. Inky's Hosting Provider is identified in the Agreement and Customer will be notified of other Sub-processors in Annex 1 or amendments thereto or otherwise in writing upon Customer's request.

(b) Where Inky sub-contracts any of its rights or obligations concerning Personal Data, including to any affiliate or Sub-processor, Inky will (i) take steps to select and retain subcontractors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent with Data Protection Laws; and (ii) enter into a written agreement with each subcontractor that imposes obligations on the subcontractor that are no less restrictive than those imposed on Inky under this DPA.

(c) If Inky provides notice to Customer of a proposed change to subcontractors or Sub-processors, Customer shall raise any objection to the appointment thereof within ten (10) days of Inky's notice to Customer. In the event Customer objects to a new subcontractor or Sub-processor, Inky will use reasonable efforts to make available to Customer a change in the services or recommend a commercially reasonable change to Customer' use of the services by the objected-to subcontractor or Sub-processor.

8. **Data Transfers**. In the event that Customer transfers Personal Data of Data Subjects located in the European Economic Area to Inky in the United States, Inky agrees to be bound by the standard contractual clauses for the transfer of personal data to processors established in third countries (Commission Decision 2010/87/EC) ("***Model Clauses***") attached hereto as Annex 1. In case of conflict between the Model Clauses and this DPA, the Model Clauses will prevail. The Model Clauses shall not apply where Inky Processes Personal Data (i) in a country that the European Commission has decided provides adequate protection for Personal Data and (ii) shall not apply to any Processing by Inky of Personal Data that is not subject to GDPR.

9. **Return or Destruction of Personal Data**. Except to the extent required otherwise by Data Protection Laws, Inky will return to Customer and/or securely destroy all Personal Data upon (a) written request of Customer or (b) termination of the Agreement. Except to the extent prohibited by Data Protection Laws, Inky will inform Customer if it is not able to return or delete any Personal Data. Any remaining Personal Data which is not deleted or effectively anonymized will be unavailable for any further Processing except to the extent required by applicable laws, including but not limited to Data Protection Laws.

10. **Governing Law, Indemnification, Limitation of Liability**. Except as required by the Model Clauses for such Personal Data as and when subject thereto, the governing law, indemnification obligations and limitations of damages and liability arising out of or related to this DPA are subject to the provisions applicable thereto in the Agreement.

11. **Term**. The effective date of this DPA shall be the date on which the term of the Agreement commences. The provisions of this DPA survive the termination or expiration of the Agreement for so long as Inky or its Sub-Processors Process the Personal Data subject hereto or as otherwise agreed by the Parties in writing.

ANNEX I: STANDARD CONTRACTUAL CLAUSES (MODEL CLAUSES)

Annex 1

To INKY Data Processing Agreement

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of General Data Protection Regulation (EU) 2016/679 ("GDPR") for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection:

The entity identified as "Customer" in the DPA (the "data exporter**"**) and the entity identified as "INKY" (the "data importer") in the Inky Data Processing Agreement ("DPA") each a "Party" and together "the Parties:"

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in the GDPR on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of the GDPR;

(d) *'the sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organizational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of

Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1

to INKY DPA Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties. By you agreeing to the Agreement, the parties will be deemed to have signed this Appendix 1.

Data exporter

The data exporter is the entity identified as "Customer" in the DPA.

Data importer

The data importer is the entity identified as "Inky" in the DPA.

Data Subjects

Data subjects include the data exporter's personnel, representatives, contractors, partners, vendors, and persons of interest.

Categories of data

The Personal Data which is Processed by the data importer through the data exporter's use of the Platform as described in the Agreement. The data exporter determines the types of data per each Service used.

Processing operations

The Personal Data transferred will be subject to the processing activities required for performance of the Platform by data importer pursuant to the Agreement between them. Data importer may use Sub-processors in connection with its Processing activities for data exporter. The initial Sub-processor is as follows:

Name of Sub-processor	Role of Sub-processor	Location
Amazon Web Services (AWS)	Hosting Provider	United States
Amazon Web Services (AWS)	Disaster Recovery	Canada
Microsoft Azure	Hosting Provider	United States
Trinity Cyber, Inc.	Attachment Scanning	United States

Appendix 2

To Inky DPA Standard Contractual Clauses

Security Measures

Description of the technical and organizational security measures implemented by INKY in its provision of the Platform to Customer under the Agreement:

1. Security.

1.1. Security Management System.

(a) **Organization.** Processor designates qualified security personnel whose responsibilities include development, implementation, and ongoing maintenance of the Information Security Program.

(b) **Policies.** The data importer's executive management reviews and supports all security related policies to ensure the security, availability, integrity and confidentiality of Personal Data. These policies are updated at least once annually.

(c) **Assessments.** Processor engages a reputable independent third-party to perform risk assessments of all systems containing Personal Data at least once annually.

(d) **Risk Treatment.** Processor maintains a formal and effective risk treatment program to identify and protect against potential threats to the security, integrity or confidentiality of Personal Data.

(e) **Sub-processor Management.** Processor maintains a formal and effective sub-processor management program.

(f) **Incident Management.** Processor reviews security incidents regularly, including effective determination of root cause and corrective action.

2. Personnel Security.

2.1. Processor personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Processor conducts reasonably appropriate criminal background checks on any employees who will have access to Personal Data under this Agreement, to the extent legally permissible and in accordance with applicable local labor law, customary practice and statutory regulations.

2.2. Personnel are required to execute a confidentiality agreement in writing at the time of hire and to protect Personal Data at all times. Personnel must acknowledge receipt of, and compliance with, Processor's confidentiality, privacy and security policies. Personnel are provided with privacy and security training on how to implement and comply with the Information Security Program. Personnel handling Personal data are required to complete additional requirements appropriate to their role (e.g., certifications). Processor's personnel will not process Personal data without authorization.

3. Access and Site Controls.

3.1 Hosting Provider Security Measures. Description of the technical organizational security measures implemented by the Sub-processor processing Personal Data, which Processor is subject to in all respects, is included in the data processing addendum linked to below. The security standards in the Sub-processor's data processing addendum provided in the link below are incorporated by reference, as amended from time to time by the Sub-processor or as replaced by a substitute Sub-processor, subject to the obligations of Processor in the Agreement when replacing Sub-processors:

https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

3.2. Access Control.

(a) **Access Management.** Processor maintains a formal access management process for the request, review, approval and provisioning of all personnel with access to Personal Data to limit access to Personal Data and systems storing, accessing or transmitting Personal Data to properly authorized persons having a need for such access. Access reviews are conducted periodically (no less than annually) to ensure that only those personnel with access to Personal Data still require it.

(b) **Infrastructure Security Personnel.** Processor has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Processor's infrastructure security personnel are responsible for the ongoing monitoring of Processor's security infrastructure, the review of the Platform, and for responding to security incidents.

(c) **Access Control and Privilege Management.** Processor's and Client's administrators and end users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Platform. Each application checks credentials in order to allow the display of data to an authorized user or administrator.

(d) **Internal Data Access Processes and Policies – Access Policy.** Processor's internal data access processes and policies are designed to protect against unauthorized access, use, disclosure, alteration or destruction of Personal Data. Processor designs its systems to only allow authorized persons to access data they are authorized to access based on principles of "least privileged" and "need to know", and to prevent others who should not have access from obtaining access. Processor employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Processor requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with Processor's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies follow industry standard practices. These standards include password complexity, password expiry, password lockout, restrictions on password reuse and re-prompt for password after a period of inactivity.

4. Data Center & Network Security.

4.1 Data Centers.

(a) **Server Operating Systems.** Processor's servers are customized for the application environment and the servers have been hardened for the security of the Platform

(b) **Disaster Recovery.** Processor replicates data over multiple systems to help to protect against accidental destruction or loss. Processor has designed and regularly plans and tests its disaster recovery programs.

(c) **Security Logs.** Processor's systems have logging enabled to their respective system log facility in order to support the security audits, and monitor and detect actual and attempted attacks on, or intrusions into, Processor's systems.

(d) **Vulnerability Management.** Processor performs regular vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis, with Critical, High and Medium security patches for all components installed as soon as commercially possible.

4.2. Networks & Transmission.

(a) **Data Transmission.** Transmissions between data centers are designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Processor transfers data via Internet standard protocols.

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

(c) **Intrusion Detection.** Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Processor intrusion detection involves:

(i) Tightly controlling the size and make-up of Processor's attack surface through preventative measures; and

(ii) Employing intelligent detection controls at data entry points.

(d) **Incident Response.** Processor maintains incident management policies and procedures, including detailed security incident escalation procedures. Processor monitors a variety of communication channels for security incidents, and Processor's security personnel will react promptly to suspected or known incidents, mitigate harmful effects of such security incidents, and document such security incidents and their outcomes.

(e) **Encryption Technologies.** Processor makes HTTPS encryption (also referred to as SSL or TLS) available.