DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its schedules and appendices (collectively, the "**DPA**"), forms part of the Master Subscription Agreement or other written agreement between Inkit and the Customer (the "**Agreement**") for the purchase of Inkit's Services.

By entering into the Agreement, the Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, its Authorized Affiliates, if and to the extent Inkit processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only and except where indicated otherwise, the term "Customer" includes the Customer and its Authorized Affiliates. All capitalized terms not defined in this DPA have the meanings given to them in the Agreement.

In the course of providing the Services to the Customer pursuant to the Agreement, Inkit may Process Personal Data on behalf of the Customer, and the Parties hereby agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

DEFINITIONS.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Authorized Affiliate**" means any of the Customer's Affiliates that (1) is subject to the European Data Protection Legislation and (2) is permitted to use the Services pursuant to the Agreement.

"**CCPA**" means the California Consumer Privacy Act 2018, Cal. Civ. Code § 1798.100, *et seq.*, and its implementing regulations, as the same may be amended from time to time.

"**Controller**" means the entity that determines the purposes and means of the Processing of Personal Data.

"**Customer Data**" has the meaning given to it in the Agreement, to the extent that such data contains Personal Data.

"**Data Protection Laws and Regulations**" means all laws and regulations, including European Data Protection Legislation and CCPA, applicable to a Party in its use or provision of the Services in connection with the Processing of Personal Data under the Agreement.

"**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates.

"**Data Subject Right**" means any right afforded to a Data Subject under Data Protection Laws and Regulations, including the rights to access, rectify, and restrict the Processing of Personal Data, to erasure (including the right to be forgotten), to data portability, to object to the Processing of Personal Data, and to not be subject to automated individual decision-making.

"European Data Protection Legislation" means (1) the EU GDPR, (2) the UK GDPR, (3) the UK Data Protection Act 2018, (4) any laws that implement such laws, (5) any laws that replace, extend, re-enact, consolidate, or amend any of the foregoing, and (6) any other legislation or regulatory requirements in force from time to time in the United Kingdom or the European Economic Area that apply to a Party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

"European Economic Area" means the member states of the European Union, Iceland, Liechtenstein, and Norway.

"EU GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Lawful Transfer Mechanism" means such legally enforceable mechanism(s) for transfers of Personal Data to third countries as may be permitted under European Data Protection Legislation from time to time.

"Personal Data Breach" means a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed by Inkit or its Sub-Processors in connection with the Agreement, of which Inkit becomes aware.

"Processing" means any operation or set of operations that is performed on Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, otherwise making available, alignment, combination, restriction, erasure, or destruction. "Process" has the corelative meaning.

"Processor" means the entity that Processes Personal Data on behalf of the Controller.

"Security, Privacy, and Architecture Datasheet" means the Security, Privacy, and Architecture Datasheet for the Services attached to this DPA as Schedule 1, as may be updated from time to time.

"Sensitive Personal Information" means Personal Data revealing: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic and biometric data processed for the purpose of uniquely identifying a natural person; data concerning health or a natural person's sex life or sexual orientation; and Personal Data relating to criminal convictions and offenses.

"**Standard Contractual Clauses"** means, (1) where the EU GDPR applies the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to third countries, as set out in the Annex to Commission Decision (EU) 2021/914, available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en or such alternative clauses as may be approved by the European Commission from time to time ("**EU SCCs**"), and (2) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("**UK SCCs**"). The Parties acknowledge that, as at the date of the Agreement, the UK SCCs approved by the UK Supervisory Authority for transfers from the United Kingdom to third countries are the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), set out in the Annex to Commission Decision 2010/87/EU, as amended to apply in a UK context (without changing the legal meaning), a copy of which has been made available by the UK Supervisory Authority at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/sccs-after-transition-period/.

"**Sub-Processor"** means any Processor engaged by Inkit to Process Customer Data.

"**Supervisory Authority"** means, (1) in the United Kingdom, the Information Commissioner's Office, or any other independent regulatory authority responsible for administering compliance with Data Protection Laws and Regulations in the United Kingdom, and (2) in the European Union, an independent public authority that is established by an EU member state pursuant to the EU GDPR.

"**UK GDPR**" has the meaning given to it in Section 3(10) (as supplemented by Section 205(4)) of the UK Data Protection Act 2018.

1. PROCESSING OF PERSONAL DATA.

1.1. **Roles of the Parties; Details of Processing.** The Parties hereby acknowledge and agree that: (1) with regard to the Processing of Personal Data, the Customer is the Controller and Inkit is the Processor; and (2) Inkit will engage Sub-Processors pursuant to the requirements set forth in Section 4 (Sub-Processors) below. The subject matter of Processing of Personal Data by Inkit is the provision of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, and the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Details of the Processing) to this DPA.

1.2. **Customer's Processing of Personal Data.** The Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For clarity, the Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. The Customer has sole responsibility for the accuracy, quality, and legality of the Personal Data and the means by which the Customer acquired the Personal Data.

1.3. **Inkit's Processing of Personal Data.** Inkit shall treat Personal Data as Confidential Information and shall (subject to the potential requirement described in the following sentence) only Process Personal Data on behalf of the Customer and in accordance with the Customer's documented instructions for the following purposes: (1) Processing in accordance with this DPA, the Agreement, and applicable Order Forms; (2) Processing initiated by users of the Customer's account in their use of the Services;

and (3) Processing to comply with other documented reasonable instructions provided by the Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. Notwithstanding the foregoing, if Inkit is otherwise required to Process Personal Data differently to comply with European Data Protection Legislation to which Inkit is subject, Inkit shall inform the Customer of that legal requirement before Processing, unless that law prohibits Inkit from doing so. Inkit will Process Personal Data in compliance with applicable Data Protection Laws and Regulations, provided that Inkit will not be in violation of this contractual obligation if Inkit's Processing of Personal Data in non-compliance with applicable Data Protection Laws and Regulations is due to the Customer.

2. RIGHTS OF DATA SUBJECTS.

2.1. **Data Subject Requests.** Inkit shall, to the extent legally permitted and to the extent Inkit is able to identify that the request comes from a Data Subject whose Personal Data was submitted to the Services by the Customer, promptly notify the Customer if Inkit receives a request from a Data Subject in relation to the exercise of any Data Subject Right ("**Data Subject Request**"). Inkit shall not respond to a Data Subject Request without the Customer's prior written consent, except to acknowledge receipt of such request and confirm that such request relates to the Customer, to which the Customer hereby agrees. Taking into account the nature of the Processing, Inkit shall assist the Customer by providing appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfillment of the Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

3. INKIT PERSONNEL.

3.1. **Confidentiality.** Inkit shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Inkit shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4. SUB-PROCESSORS.

4.1. **Appointment of Sub-Processors.** The Customer acknowledges and agrees that: (1) Inkit's Affiliates may be retained by Inkit as Sub-Processors; and (2) Inkit and Inkit's Affiliates respectively may engage third-party Sub-Processors in connection with the provision of the Services. Inkit or an Inkit Affiliate has entered into a written agreement with each Sub-Processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-Processor.

4.2. **List of Current Sub-Processors and Notification of New Sub-Processors.** A current list of Sub-Processors engaged by Inkit in the provision of the Services is available to the Customer at www.inkit.com/legal#Sub-Processors. Such Sub-Processor list includes the identities of those Sub-Processors, their country of location, and the type of processing they perform. Inkit shall provide, through the aforementioned URL, a mechanism for the Customer to subscribe to notifications of any new Sub-Processors that will Process Personal Data in connection with the Services and the Customer shall subscribe to such notifications. Provided that the Customer subscribes, Inkit shall send to the Customer notification of any new Sub-Processor prior to authorizing such Sub-Processor to Process Personal Data in connection with the Services.

4.3. **Objection Right for New Sub-Processors.** The Customer has the right to reasonably object to Inkit's use of a new Sub-Processor (e.g., where using such new Sub-Processor would weaken the protections for the Customer Data) by notifying Inkit promptly in writing within 10 business days after Inkit's issuance of the notice in accordance with Section 4.2. In the event the Customer objects to a new Sub-Processor, Inkit will use reasonable efforts to make available to the Customer a change in the Services or recommend a commercially reasonable change to the Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-Processor without unreasonably burdening the Customer. If Inkit is unable to make available such change within a reasonable period of time, which shall not exceed 30 days, the Customer has the right to terminate the applicable Order Form(s) with respect only to those Services that cannot be provided by Inkit without the use of the objected-to new Sub-Processor, by providing written notice to Inkit. Inkit will refund to the Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on the Customer.

4.4. **Liability for Sub-Processors.** Inkit is liable for the acts and omissions of its Sub-Processors to the same extent Inkit would be liable if performing the services of each Sub-Processor directly under the terms of this DPA.

5. SECURITY.

5.1. **Controls for the Protection of Customer Data.** Inkit shall maintain appropriate technical and organizational measures for protection of the security (including protection against Personal Data Breach), confidentiality, and integrity of the Customer Data, as set forth in the Security, Privacy, and Architecture Datasheet attached hereto as Schedule 1. Inkit regularly monitors compliance with these measures. The Customer is responsible for reviewing the information made available by Inkit relating to data security and making an independent determination as to whether the Services meet the Customer's requirements and legal obligations under Data Protection Laws and Regulations. The Customer acknowledges that the security measures described within the Security, Privacy, and Architecture Datasheet are subject to technical progress and development and that Inkit may update or modify such document from time to time, provided that such updates and modifications do not result in a material decrease of the overall security of the Services during the Term.

5.2. **Customer Data Incident Management and Notification.** Inkit maintains the security incident management policies and procedures specified in the Security, Privacy, and Architecture Datasheet and shall notify the Customer without undue delay after becoming aware of a Personal Data Breach in connection with the Services. In such event, Inkit shall provide information to the Customer necessary to enable the Customer to comply with its obligations under Data Protection Laws and Regulations. The content of such communication to the Customer will: (1) include the nature of Processing and the information available to Inkit; and (2) take into account that, under applicable Data Protection Laws and Regulations, the Customer may need to notify regulators or individuals of the following: (i) a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of individuals concerned, and the categories and approximate number of Personal Data records concerned; (ii) a description of the likely consequences of the Personal Data Breach; and (iii) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Inkit shall make commercially reasonable efforts to identify

the cause of such Personal Data Breach and take those steps as Inkit deems necessary and reasonable in order to remediate the cause of such Personal Data Breach to the extent the remediation is within Inkit's reasonable control. The obligation to remediate the cause of a Personal Data Breach does not apply to Personal Data Breaches that are caused by the Customer, users of the Customer's account, or third-party Vendors.

5.3. **Third-Party Certifications and Audits.** Inkit has obtained the third-party certifications and audits set forth in the Security, Privacy, and Architecture Datasheet. Upon the Customer's written request at reasonable intervals and subject to the confidentiality obligations set forth in the Agreement, Inkit shall allow for and contribute to audits and inspections ("**Audits**") conducted by the Customer (or the Customer's independent, third-party auditor that is not a competitor of Inkit and that is subject to confidentiality obligations substantially similar to those set forth in the Agreement) by providing any information regarding Inkit's compliance with the obligations set forth in this DPA in the form of a copy of Inkit's then most recent third-party audits or certifications, as applicable, that Inkit makes available to its customers generally. The Customer may perform an Audit remotely or on-site, up to one time per year, with at least three-week advance written notice, unless otherwise required by the Customer's regulators or applicable law. If the Customer requests an on-site Audit, the following terms apply: (1) such Audit will be limited to facilities operated by Inkit and shall not exceed one business day; (2) before the commencement of any such on-site Audit, the Customer and Inkit will mutually agree upon the scope and timing of the Audit; (3) the Customer shall reimburse Inkit for actual expenses and costs incurred in connection with such Audit; and (4) the Customer shall promptly notify Inkit with information regarding any non-compliance discovered during the course of an Audit.

6. RETURN AND DELETION OF CUSTOMER DATA.

6.1. Inkit shall permit the Customer to export its Customer Data as set forth in the Agreement and shall delete the Customer Data in accordance with the Agreement, applicable laws, and the Security, Privacy, and Architecture Datasheet.

7. AUTHORIZED AFFILIATES.

7.1. **Relationship between Inkit and Customer's Authorized Affiliates.** The Parties acknowledge and agree that, by executing the Agreement, the Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing an independent DPA between Inkit and each such Authorized Affiliate, subject to the provisions of the Agreement and this Section 7 and Section 8. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For clarity, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to this DPA. Any access to and use of the Services by Authorized Affiliates must comply with the terms of the Agreement and any violation of the terms of the Agreement by an Authorized Affiliate shall be deemed a violation by the Customer.

7.2. **Communication.** The Customer that is the contracting party to the Agreement will remain responsible for coordinating all communication with Inkit under this DPA and shall make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

7.3. **Rights of Authorized Affiliates.** Where an Authorized Affiliate enters into a DPA with Inkit, it will, to the extent required under applicable Data Protection Laws and

Regulations, be entitled to exercise the rights and seek the remedies under this DPA, subject to the following:

7.3.1. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek a remedy under this DPA against Inkit directly by itself, each Party (and all of its Affiliates) agree that: (1) solely the Customer that is the contracting party to the Agreement will exercise any such right or seek any such remedy on behalf of the Authorized Affiliate; and (2) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together.

7.3.2. Each Party (and all of its Affiliates) agree that the Customer that is the contracting party to the Agreement shall, when carrying out an onsite Audit, take all reasonable measures to limit any impact on Inkit and its Sub-Processors by combining, to the extent reasonably possible, several Audit requests carried out on behalf of different Authorized Affiliates in one single Audit.

8. LIMITATION OF LIABILITY.

8.1. Each Party's (and all of its Affiliates') liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Inkit, whether in contract, tort, or under any other theory of liability, is subject to the "Limitation of Liability" section set forth in the Agreement, and any reference in such section to the liability of a Party means the liability of that Party and all of its Affiliates under the Agreement and all DPAs together.

9. EUROPEAN SPECIFIC PROVISIONS.

9.1. **Provision of Assistance.** Upon the Customer's request, Inkit shall provide the Customer with reasonable cooperation and assistance needed to fulfill the Customer's obligation under Articles 32 to 36 UK GDPR and EU GDPR, including, to the extent required, (1) to carry out a data protection impact assessment related to the Customer's use of the Services, to the extent the Customer does not otherwise have access to the relevant information and to the extent such information is available to Inkit, and (2) in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 9.1, to the extent required under the UK GDPR or the EU GDPR, as applicable.

9.2. **Infringement Instructions.** Inkit shall immediately inform the Customer if, in Inkit's opinion, a Customer instruction violates European Data Protection Legislation and shall be entitled to immediately cease Processing Customer Data until such instruction is withdrawn or amended to render such instruction compliant with applicable European Data Protection Legislation.

9.3. **Transfer Mechanisms for Data Transfers.** The Parties acknowledge that the performance of the Agreement may necessitate international transfers of Customer Data from Customer to Inkit.

9.3.1. **Transfers from the European Economic Area.** For transfers of Customer Data under the Agreement from the European Economic Area to countries that do not ensure an adequate level of data protection within the meaning of applicable

European Data Protection Legislation of the foregoing territories, the EU SCCs will apply, subject to Section 9.3.3 and the following:

9.3.1.1. By signing this DPA, the Parties acknowledge that the EU SCCs are incorporated into and form an integral part of this DPA;

9.3.1.2. In accordance with Section 1.1 of this DPA, Module Two of the EU SCCs will apply for the purposes of transfers of Customer Data under this Agreement. Modules One, Three, and Four of the EU SCCs will not apply;

9.3.1.3. In Clause 7, the optional docking clause will apply;

9.3.1.4. In Clause 9, Option 2 will apply, and the period for prior notice of Sub-Processor changes shall be as set out in Section 4.3 of this DPA;

9.3.1.5. In Clause 11, the optional language will not apply;

9.3.1.6. Clause 12(a) of the EU SCCs will be subject to the limitation of liability provisions set out in the Agreement;

9.3.1.7. In Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws of Ireland;

9.3.1.8. In Clause 18(b), disputes will be resolved by the courts of Ireland;

9.3.1.9. Annex I of the EU SCCs will be deemed completed with the information set out in Schedule 2 to this DPA; and

9.3.1.10. Annex II of the EU SCCs will be deemed completed with the information set out in Schedule 1 to this DPA.

9.3.2. Transfers from the United Kingdom. For transfers of Customer Data under the Agreement from the United Kingdom to countries that do not ensure an adequate level of data protection within the meaning of applicable Data Protection Legislation and Regulations, the UK SCCs will apply, subject to Section 9.3.3 and the following:

9.3.2.1. By signing this DPA, the Parties acknowledge that the UK SCCs are incorporated into and form an integral part of this DPA.

9.3.2.2. Inkit shall be the “data importer” and the Customer shall be the “data exporter”.

9.3.2.3. (1) Copies of Sub-Processor agreements provided by Inkit to the Customer pursuant to Clause 5(j) of the UK SCCs may be redacted to the extent necessary to protect commercial information, business secrets, and other confidential information, (2) clauses unrelated to the UK SCCs may be removed by Inkit beforehand; and (3) such copies will be provided by Inkit, in a manner to be determined in its discretion, only upon request by the Customer.

9.3.2.4. Appendix I of the UK SCCs will be deemed completed with the information set out in Schedule 2 to this DPA; and

9.3.2.5. Appendix 2 of the UK SCCs will be deemed completed with the information set out in Schedule 1 to this DPA.

9.3.3. Additional terms to the Standard Contractual Clauses. The following additional terms will apply to the Standard Contractual Clauses:

9.3.3.1. The scope of instructions set out in Section 1.3 of this DPA will apply for the purposes of Clause 5(a) of the UK SCCs and Clause 8.1(a) of the EU SCCs.

9.3.3.2. Pursuant to Clause 5(h) of the UK SCCs and Clause 9(a) of the EU SCCs, the Customer acknowledges and agrees that Inkit has the right to engage Sub-Processors in accordance with the process described in Section 4 of this DPA.

9.3.3.3. Audits described in Clauses 5(f) and 12(2) of the UK SCCs and Clauses 8.9(c) and (d) of the EU SCCs will be carried out in accordance with the provisions of Section 5.3 of this DPA.

9.3.3.4. The certification of deletion of Personal Data described in Clause 12(1) of the UK SCCs and Clauses 8.5 and 16(d) of the EU SCCs will be provided by Inkit to the Customer only upon the Customer's request.

9.3.4. The Customer shall accept any modifications to the Standard Contractual Clauses entered into between Inkit and the Customer (where applicable) that are necessary to comply with applicable European Data Protection Legislation. If the Standard Contractual Clauses are replaced, amended, or no longer recognized as valid under European Data Protection Law, or if a relevant Supervisory Authority or European Data Protection Legislation requires either Party to adopt an alternative transfer solution, the Parties shall work together in good faith to put an alternative Lawful Transfer Mechanism in place to ensure the processing continues to comply with European Data Protection Legislation.

9.3.5. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

9.3.6. Onward Transfers. The Customer authorizes Inkit to transfer Customer Data to Sub-Processors engaged in accordance with Section 4, provided, however, that, to the extent required under European Data Protection Legislation, such transfers are effected by way of a Lawful Transfer Mechanism.

10. CALIFORNIA CONSUMER PRIVACY ACT OF 2018.

10.1. The following shall apply to the extent the Customer is subject to the CCPA:

10.1.1. All references to Data Protection Laws and Regulations in this DPA shall be deemed to include a reference to the CCPA;

10.1.2. All references to Personal Data in this DPA shall be deemed to include Personal Information, as defined in the CCPA, provided such data is Customer Data;

10.1.3. All references to "Controller" in this DPA shall also be deemed to be references to "**Business**," as defined in the CCPA;

10.1.4. All references to "Processor" in this DPA shall also be deemed to be references to "**Service Provider**," as defined in the CCPA;

10.1.5. Any capitalized term used in this Section 10 but not defined herein shall have the meaning set forth in the CCPA.

10.2. Inkit shall not Sell any Personal Information.

10.3. Inkit shall Process Personal Information solely as set forth in Section 1.3 (the "**Business Purpose**") and shall not retain, use, or disclose the Personal Information for any purpose other than the Business Purpose.

10.4. Inkit does not receive any Personal Information from the Customer as consideration for Inkit's provision of the Services.

10.5. Inkit certifies that it understands the restrictions set forth in this Section 10 and will comply with them.

List of Schedules

Schedule 1: Inkit's Security, Privacy, and Architecture Datasheet
Schedule 2: Details of the Processing

SCHEDULE 1

Inkit Security, Privacy, and Architecture Information Security Datasheet
(effective as of November 2021; subject to change without notice)

Introduction. The purpose of this document is to provide high-level information to Inkit's customers regarding Inkit's commitment to security and data protection.

Inkit's Corporate Trust Commitment. Inkit is committed to achieving and maintaining the trust of its customers. Inkit's goal is to be as transparent as possible with its customers in offering security and similar protections to meet and even exceed expectations in today's modern computing world.

General Policy. Inkit has a documented information security policy that all employees must read and acknowledge. This policy is reviewed and updated annually. Security policy development, maintenance, and issuance is the responsibility of Inkit's CTO.

Inkit's Infrastructure. Inkit currently hosts the Services in the United States with Google Cloud Platform in its US-Central data center. For customers who have their Customer Data stored in Europe, that is hosted with Google Cloud Platform in its Belgium data center.

Third-Party Architecture. Inkit may use one or more third-party content delivery networks to provide the Services and to optimize content delivery via the Services. Content items to be served to subscribers or end-users, such as images or attachments uploaded to the Services, may be cached with such content delivery networks to expedite transmission. Information transmitted across a content delivery network may be accessed by that content delivery network solely to enable these functions.

Audits, Certifications, and Regulatory Compliance. Inkit is planning ISO 27001 and SOC 2 compliance. Inkit also self-certifies to the EU-US and Swiss-US Privacy Shield Frameworks and is HIPAA compliant.

Technical and organizational measures taken by Inkit's Sub-Processors. Before engaging Sub-Processors, Inkit performs due diligence on the security and privacy practices of its Sub-Processors to ensure they provide a level of security appropriate to their access to data and the scope of the services they are engaged to provide. Upon completion of this assessment, the Sub-Processor is required to enter into appropriate data protection, security, and confidentiality provisions in its contract with Inkit.

Security Controls.

1. *Organization Security.* Inkit's CTO is responsible for the overall security of the Services, including oversight and accountability. Inkit's contracts with third-party hosting providers include industry-standard information protection requirements.

2. *Asset Classification and Logical Access Control.* Inkit maintains an inventory of essential information assets, such as servers, databases, and information. All Customer Data is classified by Inkit as confidential. All Inkit servers run Ubuntu LTS. Inkit adopts the principle of least privilege for all accounts running application or database services, as well as with its own staff. For example, Inkit's customer account managers only have access to the regions for which they are directly responsible. Inkit maintains separate development, staging (or sandbox), user acceptance testing, and production environments. Access to each environment and within each environment is strictly

controlled. Access to Inkit's servers are controlled via revocable SSH keys managed via configuration management and rotated at least annually. All accessing of Inkit's servers or Customer Data is logged and can only be accessed through Inkit's VPN, which uses multi-factor authentication. Database access is controlled via 32- and 64-character password. Inkit's HR onboarding and off-boarding processes handle provisioning and de-provisioning of accounts and access.

3. *Personnel Security.* All Inkit employees sign confidentiality agreements when their employment begins. Inkit conducts background checks of its employees as part of its onboarding process. All Inkit employees are informed of and agree to comply with Inkit's security policies and practices as a part of their initial onboarding. System administrators, developers, and other users with privileged usage receive special and ongoing training and are subjected to additional background screening.

4. *Physical and Environmental Security.* Access to Inkit facilities is controlled by 24-hour security. All Inkit offices are protected by locked access and are under 24-hour video surveillance. All Inkit employee workstations are encrypted and password protected, and all Inkit user accounts require two-factor authentication. Data centers and servers are managed and controlled by Google Cloud Project. Details on the security applicable to these facilities can be found at https://cloud.google.com/terms/data-processing-terms. Inkit employees have no access to any of these data centers.

5. *Policies and Logging.* The Services are operated pursuant to the following procedures to enhance security:

    - User passwords are never transmitted in clear text and use industry-standard hashing functions to determine password validity;
    - API key information for third-party services provided by the customer are encrypted for storage;
    - Inkit keeps audit logs for all access to production servers;
    - Server access is controlled via public key access instead of using passwords. Server access is only permitted while on VPN that requires multi-factor authentication;
    - Logs are stored in a secure centralized host to prevent tampering;
    - Inkit application and ssh audit logs are stored for one year;
    - Passwords are not logged under any circumstances;
    - Access to Inkit mail and document services is only allowed on approved mobile devices that have automated security policies enforced, such as encryption, autolock, and password;
    - All access to customer dashboard accounts by Inkit employees must be done via an internal service that is accessible only via a three factor VPN. As part of Inkit's information security policy, employees may not store any Customer Data on removable media.

6. *Intrusion Detection.* Inkit monitors system, user, and file behavior across its infrastructure using a host-based intrusion detection system. Alerts are monitored by Inkit's security team 24/7. Additionally, Inkit may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Services function properly.

7. *Security Logs.* All Inkit systems used in the provision of the Services, including firewalls, routers, network switches, and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis. Inkit has automated alerts and searches for such logs.

8. *System Patching and Configuration Management.* Inkit patches its servers and rebuilds its entire cloud infrastructure from configuration management systems on a regular basis, which ensures that the latest patches are applied and that Inkit "resets" back to a known, clean state. Inkit's configuration management system regularly applies patches via Linux repositories. Inkit uses Chef configuration management tool to automate this entire process and its entire infrastructure. Inkit maintains multiple environments and tests all changes in containerized development environments and in live staging environments before making changes to production environments.

9. *Vulnerability Management.* Inkit's infrastructure and applications are continuously scanned by a vulnerability management system. Alerts are monitored and addressed monthly by Inkit's security team. Inkit also maintains a list membership to various CVE vulnerability mailing lists. Patches and critical and high vulnerabilities are remediated no later than 30 days following discovery. Inkit uses static code analysis tools during the build process (such as Brakeman and bundler-audit) to perform static security analysis.

10. *Third-Party Penetration Testing.* Inkit undergoes a third-party penetration test of the Services on an annual basis.

11. *Monitoring.* For technical monitoring, maintenance, and support processes, Inkit uses a combination of tools to ensure that processes and servers are running properly, including but not limited to:

    - Process monitoring;
    - CPU, disk, and memory monitoring;
    - Uptime monitoring;
    - Functional monitoring;
    - Database monitoring;
    - APM performance monitoring; and
    - Error monitoring.

12. *Customer Access Control.* The Services include a variety of security controls. These controls include:

    - API IP Whitelistin – defines the range of IP addresses from which a customer's user can access Inkit's APIs to prevent unauthorized third parties from accessing the Services;
    - Dashboard Account IP Whitelisting – defines a range of IP addresses from which a customer's user can access the Inkit dashboard to prevent unauthorized parties from accessing the Services
    - Single-sign on with a Google Account – customers can access the Services by means of a Google Account, which allows customers to configure such access to require two-factor authentication;
    - Single-sign on via Auth0 – customers can access the Services via Auth0, which allows customers to configure access via their Auth0 installation;
    - Mobile Authenticator – customers can enable two factor authentication via Authy which allows a mobile authenticator to be required for access to Inkit's dashboard;

- Customer Configurable Roles and Permissions – customers have the option to manage their users of the Services through selective permissioning;
- All requests on Inkit's dashboard have cross-site request forgery (CSRF) protection. All web services use encrypted HTTPS for all traffic and disallow all HTTP traffic via HTTP Strict Transport Security ("HSTS");
- User passwords on Inkit's dashboard must meet minimum password length requirements. At a customer's request, Inkit can add password complexity requirements, such as lowercase, uppercase, numeral, and special characters and set a password expiration policy such that the customer's users must change their passwords regularly;
- User password history of the last six passwords prevents the reuse of a customer user's password on Inkit's dashboard;
- Failed login attempts are recorded and an account is locked out with the owner notified after multiple failed attempts.

13. *Development and Maintenance.* Inkit uses tools such as GitHub and Jenkins to effectively manage the development lifecycle. During testing, Inkit generates sandbox accounts and fake data for testing. Inkit does not use production data in sandbox accounts. Application source control is provided using private GitHub repositories. Inkit has controls in place to ensure that all code must be approved before being merged to Inkit's main code branch; only the CTO and approved employees are granted access to promote code to production. Inkit developers receive additional security training as part of their onboarding and undergo regular and periodic security training during the term of their employment. Inkit maintains a list of core security principles for engineering and high-level guidelines on security topics for secure software development.

14. *Malware Prevention.* Inkit adopts the principle of least privilege for all accounts running application or database services. Proper change management ensures that only authorized packages are installed via a package management system containing only trusted software, and that software is never installed manually. All Inkit employee computers have virus scanners installed and updated definitions sent out from a central device management platform.

15. *Information Security Incident Management.* Inkit maintains security incident management policies and procedures. Inkit has 24x7x365 on-call incident management staff. Inkit uses tools such as PagerDuty to ensure complete coverage with defined escalation policies. Inkit maintains a security incident response plan to be enacted in the event of an incident.

16. *Data Encryption.* The Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Services, including 256-bit TLS Certificates and 4096-bit RSA public keys at a minimum. Inkit audits the TLS ciphers used in connection with the provision of the Services with third-party security auditors to ensure that anonymous or weak ciphers are not used. Such audits also confirm that the Services do not allow client renegotiation, support downgrade attack protection and forward secrecy. Data that is shipped to Google Cloud Platform is encrypted in transit and also at-rest using AES-256 encryption via Google's managed encryption key process. Where use of the Services requires a customer to provide access to third-party services (e.g., an API key to access a customer's email service provider to enable the sending of email through the Inkit Services), Inkit performs additional encryption of that information.

17. *Return and Deletion of Customer Data.* The Services allow import, export, and deletion of Customer Data by authorized users at all times during the term of a customer's subscription, subject to the terms of the Agreement. Following termination or expiration of the Services, Inkit securely overwrites or deletes Customer Data within 60 days following any such termination, in accordance with the Agreement, applicable laws, and the Documentation.

18. *Reliability and Backup.* All networking components, SSL accelerators, load balancers, web servers, and application servers are configured in a redundant configuration. All Customer Data submitted to the Services is stored on a primary database server with multiple active clusters for higher availability. All database servers replicate in near real-time and are backed up on a regular basis. Backups stored on backup media are encrypted using AES-256 encryption. Backups are verified for integrity.

19. *Business Continuity Management and Disaster Recovery.* Inkit has a written business continuity and disaster recovery plan, which is tested annually. Inkit has tested database backups and failovers as part of such plan. Backups are encrypted and stored in Google Cloud Platform provided backup services.

20. *Mobile Device Management Policies.* Inkit uses Mobile Device Management ("MDM") platforms to control and secure access to Inkit resources on mobile devices such as phones, tablets, and laptops. Inkit uses Rippling for its phone and tablet MDM policy and enforces common security settings such as, but not limited to, encryption, lock screen passwords, password expiration, display timeouts, and remote location and remote wipe. Furthermore, Inkit uses Rippling for laptop and desktop management to enforce common security settings, including, but not limited to, hard disk encryption, security patches, and remote location and remote wipe capabilities.

21. *Contacts.* Inkit's security team can be reached at security@inkit.com.

SCHEDULE 2

Details of the Processing

A. LIST OF PARTIES

Data exporter(s):

Name: The Customer listed in the Agreement.

Address: The Customer's address listed in the Agreement.

Contact person's name, position, and contact details: The contact person identified in the Agreement

Activities relevant to the data transferred under these Clauses: Inkit provides the Services to the Customer in accordance with the Agreement.

Signature and date: The Parties agree that execution of the Agreement will constitute execution of this Schedule by both Parties.

Role (controller/processor): Controller

Data importer(s):

Name: Inkit.

Address: Inkit's address listed in the Agreement.

Contact person's name, position, and contact details: Contact details for Inkit are specified in the Agreement. The team responsible for data protection can be contacted at legal@inkit.com.

Activities relevant to the data transferred under these Clauses: Inkit provides the Services to the Customer in accordance with the Agreement.

Signature and date: The Parties agree that execution of the Agreement will constitute execution of this Schedule by both Parties.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

Nature and Purpose of Processing.

Inkit will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation and as further instructed by the Customer in its use of the Services.

Duration of Processing and Frequency of Transfer.

Subject to Section 6 of the DPA, Inkit will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects.

The Customer may submit Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

1. Prospects, customers, business partners, and vendors of the Customer (who are natural persons);

2. Employees or contact persons of the Customer's prospects, customers, business partners, and vendors;

3. Employees, agents, advisors, and freelancers of the Customer (who are natural persons);

4. Customer users that are authorized by the Customer to use the Services.

Type of Personal Data.

The Customer may submit Personal Data to the Services in accordance with the terms of the Agreement, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

1. First and last name;

2. Contact information (e.g., email, phone, mailing address);

3. Device data;

4. ID data;

5. Personal life data.

Special Categories of Data.

Unless otherwise specifically agreed upon in advance in writing between the Parties, the Customer shall not use the Services to Process any Sensitive Personal Information.

Transfers to Sub-Processors.

The transfer to Sub-Processors is as described at www.inkit.com/legal#Sub-Processors.

C. COMPETENT SUPERVISORY AUTHORITY

The competent Supervisory Authority for the purposes the EU SCCs shall be determined in accordance with Clause 13 EU SCCs and the EU GDPR. Where the data exporter is not established in an EU Member State and does not have to appoint a representative pursuant to Article 27(2) of the EU GDPR, the Supervisory Authority for the purposes of the EU SCCs shall be Irish Data Protection Commission. For the purposes of the UK SCCs, the Supervisory Authority shall be the Information Commissioner's Office.