Inkstamp Data Processing and Security Addendum

Document	Inkstamp Data Processing and Security Addendum (“DPA”)
Version	2026.07.16
Effective date of this version	July 16, 2026
Permanent URL	`https://inkstamp.ai/legal/dpa/2026.07.16.pdf`
Incorporated with	Inkstamp Master Services Agreement (“MSA”), in the version identified in the applicable Order Form

---

This Inkstamp Data Processing and Security Addendum states the data-protection roles, processing terms, security controls, subprocessor process, remote-access rules, Security Incident obligations, permitted and prohibited data categories, data-region commitment, retention and deletion terms, and privacy-law obligations that apply when Diorthos processes Customer Data in connection with the Inkstamp Services. This DPA forms part of the Agreement between **Diorthos LLC** (“**Diorthos**”) and Customer when incorporated through a signed Order Form.

---

1. Relationship to the MSA; Interpretation

1.1 Incorporation and version

This DPA is incorporated into the Agreement through each Order Form that identifies its version and effective date, in accordance with Sections 2.1 and 2.2 of the MSA. The version identified in an Order Form governs that Order Form throughout its Subscription Term, subject to the renewal-adoption mechanics of MSA Section 14.2(c). The only component of this DPA that changes without a new version is the Approved Subprocessor List, which is updated exclusively under Section 7 (MSA Section 2.3(b)).

1.2 Role in the order of precedence

Under MSA Section 2.4(a), this DPA controls in the event of a conflict with respect to **privacy, data processing, security incidents, subprocessors, retention, and privacy-law deletion obligations**. This DPA does not modify: the Tenant Graph Governance and Retention Schedule with respect to graph approval authority, provenance, record-class retention, export, archival, and governed destruction — this DPA states the retention and deletion *framework*, and the Tenant Graph Governance and Retention Schedule states the customer-specific *record classes, retention periods, custody selections, and destruction authority* within that framework (Section 12); a signed Negotiated Addendum with respect to the provisions of this DPA it expressly modifies; any High-Risk AI Use-Case Schedule with respect to the use it governs; the Order Form with respect to quantities, prices, the Subscription Term, selected services, and customer-specific commercial terms; the SLA with respect to availability, support, maintenance, and service credits; the Runtime Schedule with respect to responsibility for the Runtime Environment; the Product Schedule with respect to product operation, Data Stream counting, Diorthos Cloud Services, and Offline License File behavior; or the AUP with respect to permitted and prohibited use.

1.3 Definitions; interpretation

Capitalized terms used but not defined in this DPA have the meanings given in the MSA or, if not defined there, in the incorporated document in which they are defined (for example, “**Diorthos Cloud Services**,” “**Hosting Partner**,” “**Hosted Runtime**,” “**Customer-Provided Runtime**,” “**Runtime Environment**,” “**Approved Model Environment**,” “**Customer AI Account**,” and “**Local Model Environment**” are defined in the Product Schedule, and “**Runtime Responsibility Matrix**” is defined by pointer in the Product Schedule and set out in the Runtime Schedule). Section headings are for convenience only, “including” and its variants mean “including without limitation,” words importing the singular include the plural and vice versa, and the interpretation rules of MSA Section 17.10 apply to this DPA.

---

2. Definitions

“Account Data” means information that Diorthos processes for its own business operations in connection with

the Parties' relationship, including the names, business contact details, and role assignments of Customer personnel and Authorized Users used for account administration, identity and access management, Governance Role mapping, billing, and support communications; Order Form and contract records; payment records; and support tickets and correspondence.

"Applicable Data Protection Laws" means all laws and regulations applicable to a Party's Processing of Personal Data under the Agreement, including, in each case to the extent applicable to that Processing: the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020, and its implementing regulations (the "**CCPA**"); other comprehensive U.S. state privacy laws and their implementing regulations (collectively with the CCPA, "**US State Privacy Laws**"); U.S. federal privacy and data-security laws applicable to the data categories actually Processed; and, if and to the extent applicable to Customer Data, Regulation (EU) 2016/679 (the "**GDPR**") and the GDPR as incorporated into United Kingdom law (the "**UK GDPR**").

"Approved Subprocessor List" means Diorthos's then-current list of Subprocessors, published at `https://inkstamp.ai/legal/subprocessors` and updated exclusively as stated in Section 7. The Approved Third-Party Services Schedule identified in or attached to the applicable Order Form identifies which listed services (including the Hosting Partner) apply to Customer's deployment.

"Approved Third-Party Services Schedule" means the customer-specific schedule identified in or attached to the applicable Order Form that identifies the approved third-party services applicable to Customer's deployment — including the Hosting Partner, the authentication provider, the remote-access tool and any recording restriction, monitoring providers, support channels, and the approved credential-exchange method — together with, for each service, the data it may receive, its purpose, and applicable restrictions.

"Customer Data" has the meaning given in the Product Schedule: information, records, files, content, prompts, instructions, credentials, configuration details, and other data supplied by or on behalf of Customer or retrieved from Customer systems.

"Deidentified Data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, as further described under Applicable Data Protection Laws.

"Diorthos-Controlled Systems" means: (a) the Diorthos Cloud Services and the infrastructure on which they run — including Subprocessor infrastructure — and each dedicated, logically isolated tenant graph dataset; (b) the portions of a Hosted Runtime for which Diorthos, or the Hosting Partner as Diorthos's Subprocessor, is responsible under the Runtime Responsibility Matrix; (c) Diorthos's internal business and development systems to the extent they store Customer Data or Customer credentials; and (d) Diorthos-controlled credential storage. Diorthos-Controlled Systems do not include: Customer's source systems and other Customer systems; a Customer-Provided Runtime; the portions of a Hosted Runtime for which Customer is responsible under the Runtime Responsibility Matrix; a Customer AI Account or the AI provider's systems; or a Local Model Environment.

"Governed Record" has the meaning given in the Product Schedule: a committed graph statement, linked evidence, approval or rejection, authority grant, reviewer disposition, retention classification, destruction approval, or other record maintained through the governed lifecycle described in Product Schedule Section 3.3.

"Personal Data" means that portion of Customer Data that identifies, relates to, describes, or is reasonably capable of being associated or linked with an identified or identifiable natural person or household, and includes "personal information," "personal data," and equivalent terms under Applicable Data Protection Laws.

"Process" or **"Processing"** means any operation or set of operations performed on data, whether or not by automated means, including collection, recording, organization, structuring, storage, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, and destruction.

"Security Incident" means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Data Processed in Diorthos-Controlled Systems, and includes a compromise of Customer Data on a Customer-Provided Runtime to the extent arising from Diorthos's remote access under Section 6.1 or from the acts or omissions of Diorthos personnel or contractors. A Security Incident does not include an unsuccessful attempt or activity that does not result in unauthorized access to Customer Data, such as an unsuccessful log-in attempt, ping, port scan, denial-of-service attack that does not compromise Customer Data, or ordinary network probing of firewalls or edge systems.

"Subprocessor" means a third party engaged by Diorthos that Processes Customer Data on Diorthos's behalf to provide the Inkstamp Services, including the Hosting Partner. The parties and services that are *not* Subprocessors are identified in Section 7.5.

“Tenant Graph Data” has the meaning given in the Product Schedule: Customer-specific graph statements, linked evidence, Customer Content, Customer Outputs, Governed Records, and PROV-O-compatible provenance stored in the Tenant Knowledge Graph. Customer Outputs and Tenant Graph Data do not include the underlying Inkstamp Components used to generate, govern, or store them.

---

3. Roles of the Parties

3.1 Roles by Processing activity

The Parties’ roles are identified by Processing activity rather than by a single universal designation:

a. **Customer** determines the business purposes and means of Processing Customer Data and is the “controller,” “business,” or equivalent under Applicable Data Protection Laws.

b. **Diorthos** Processes Customer Data on Customer’s behalf to provide the Inkstamp Services — including operating the Diorthos Cloud Services, managing the portions of a Hosted Runtime allocated to Diorthos under the Runtime Responsibility Matrix, storing and using credentials under Section 5.3, providing remote support under Section 6, and performing Professional Services — and is the “processor,” “service provider,” or equivalent where those terms apply.

c. The **Hosting Partner** is a Subprocessor with respect to the Hosted Runtime infrastructure it provides, and each infrastructure provider from which Diorthos procures Diorthos Cloud Services infrastructure is a Subprocessor with respect to that infrastructure.

d. An **AI provider under a Customer AI Account** is a Customer-authorized third-party service acting under Customer’s own commercial arrangement with that provider (MSA Section 4.4(a)); it is not a Diorthos Subprocessor.

e. A **Local Model Environment** operates on Customer-controlled infrastructure and is not a third-party recipient of Customer Data, unless it is hosted for Customer by another provider, in which case that provider is Customer’s own vendor.

f. **Locally installed Inkstamp Components** (including Filetray and Flowbot) operating on a Customer-Provided Runtime Process Customer Data on that Customer-controlled environment as part of Customer’s own use of licensed software; Diorthos does not receive or Process that data except through the Diorthos-Controlled Systems and access described in this DPA.

g. Customer authorizes the specific transmissions, data categories, destinations, and retention classes shown in the applicable Order Form, Data Stream Schedule, and Tenant Graph Governance and Retention Schedule (MSA Section 9.2).

3.2 Account Data

Diorthos Processes Account Data as an independent controller or business for its legitimate business operations — administering the Parties’ relationship, providing and securing the Inkstamp Services, identity and access management, billing, support, and complying with law — consistent with Applicable Data Protection Laws and Diorthos’s published privacy notice. Account Data is not subject to the processor and service-provider terms of this DPA, but Diorthos will protect it using the relevant controls in Section 5 and Annex B.

3.3 Compliance with law

Each Party will comply with the obligations that apply to it under Applicable Data Protection Laws in respect of Customer Data. Customer is responsible for the lawfulness of the Processing it instructs, including all rights, consents, notices, and lawful bases needed to provide Customer Data to Diorthos and to authorize the Processing described in the Agreement (MSA Section 4.2), and for its regulatory responsibilities under MSA Section 4.6. Diorthos is responsible for the product-side functions described in Product Schedule Section 10.4 and for the security obligations for Diorthos-Controlled Systems stated in this DPA.

3.4 US State Privacy Law service-provider terms

To the extent US State Privacy Laws apply to Personal Data, Diorthos is a “service provider” or “processor” and:

a. will Process Personal Data solely for the business purposes described in Section 4.1 and the Agreement, and not for any other commercial purpose;

b. will not “sell” or “share” Personal Data (as those terms are defined in the CCPA), and will not Process Personal Data for cross-context behavioral advertising or targeted advertising;

c. will not retain, use, or disclose Personal Data outside the direct business relationship between the Parties or

for any purpose other than the business purposes described in Section 4.1, except as permitted by Applicable Data Protection Laws;

d. will not combine Personal Data with personal information that Diorthos receives from or on behalf of another person, or collects from its own interactions with individuals, except as permitted by Applicable Data Protection Laws for a service provider or processor;

e. certifies that it understands the restrictions in this Section 3.4 and will comply with them;

f. will notify Customer without undue delay if Diorthos determines that it can no longer meet its obligations under Applicable Data Protection Laws, and Customer may then take the steps described in Section 4.1(d); and

g. grants Customer the right, upon reasonable written notice, to take reasonable and appropriate steps — through the review rights in Section 14 and the cooperation obligations in Section 13 — to ensure that Diorthos's use of Personal Data is consistent with Customer's obligations, and to stop and remediate any unauthorized use of Personal Data; and

h. will comply with the obligations applicable to a service provider or processor under US State Privacy Laws and provide the same level of privacy protection as those laws require of Customer as a business or controller with respect to the Personal Data Diorthos Processes.

3.5 General processor standard

To the extent the GDPR or UK GDPR applies to Personal Data, the obligations of Diorthos under this DPA — Processing only on documented instructions (Section 4.1), personnel confidentiality (Section 4.4), security measures (Section 5 and Annex B), Subprocessor conditions and flow-down (Section 7), assistance with individual rights (Section 11), Security Incident notification (Section 8), assistance with assessments and consultations (Section 13), deletion or return at the end of services (Section 12), and information and review rights (Section 14) — are intended to satisfy the processor-contract requirements of GDPR Article 28(3), and the Parties will interpret them accordingly. Cross-border transfer mechanics are addressed in Section 15.

---

4. Processing of Customer Data

4.1 Documented instructions

a. Diorthos will Process Customer Data only on Customer's documented instructions, including with regard to disclosures and transfers, unless required to do otherwise by applicable law, in which case Diorthos will inform Customer of that legal requirement before Processing unless the law prohibits doing so on important grounds of public interest.

b. Customer's complete documented instructions are: (i) the Agreement, including this DPA, the applicable Order Form, the Data Stream Schedule, the Tenant Graph Governance and Retention Schedule, each applicable Use-Case Schedule, and each SOW; (ii) configuration and governance actions taken by Customer's Authorized Users through the Inkstamp Services, including approvals recorded through an Approval Interface; and (iii) other written instructions agreed by the Parties, which may be implemented as Professional Services if they require work beyond the standard Inkstamp Services.

c. Diorthos will inform Customer promptly (and, where the GDPR or UK GDPR applies to the affected Personal Data, immediately) if, in Diorthos's opinion, an instruction infringes Applicable Data Protection Laws, and may suspend performance of that instruction until the Parties resolve the concern. Diorthos is not obligated to perform a legal review of Customer's instructions.

d. If Diorthos notifies Customer under Section 3.4(f), or if Customer reasonably determines that Diorthos is Processing Personal Data in violation of this DPA, Customer may instruct Diorthos to stop the non-compliant Processing, and Diorthos will remediate without undue delay.

4.2 Customer-specific Processing details

The customer-specific Processing details — including data categories, affected individuals, the Approved Model Environment, the Hosting Partner, tenant graph location and region, record-class retention, and destruction authority — are identified in the Order Form, the Data Stream Schedule, and the Tenant Graph Governance and Retention Schedule (MSA Section 9.2). Annex A states the standing frame for those details.

4.3 Data-category limits

Only the data categories expressly identified in the applicable Data Stream Schedule may be transmitted to a Customer AI Account or to the Diorthos Cloud Services (MSA Section 9.3; Product Schedule Section 3.4(d)). The applicable Data Stream Schedule states the data-minimization and redaction categories for each approved data

flow, including the fields removed before model inference (Section 9.1); minimization, redaction, and related deterministic processing occur in the designated Runtime Environment (Product Schedule Section 3.4(a)).

4.4 Personnel confidentiality

Diorthos will ensure that each person it authorizes to Process Customer Data — including employees and contractors — is bound by a written confidentiality obligation or an appropriate statutory duty of confidentiality, and Processes Customer Data only as needed to perform under the Agreement.

4.5 Deidentified and aggregated data

Diorthos's use of feedback and generalized, non-customer-specific learnings is governed by MSA Section 7.6. If Diorthos Processes Deidentified Data derived from Customer Data, Diorthos will: (a) maintain and use it only in deidentified form and take reasonable measures to ensure it cannot be associated with an individual or with Customer; (b) not attempt to reidentify it, except as permitted by Applicable Data Protection Laws solely to test the effectiveness of its deidentification processes; (c) publicly commit to maintain and use it in deidentified form; and (d) contractually obligate any recipient to comply with this Section. Nothing in this Section expands the rights granted in MSA Section 7.6, including its prohibition on using Customer Content to train a general-purpose model without express written authorization.

---

5. Security

5.1 Security program; baseline controls

Diorthos will maintain a written information-security program with administrative, technical, and physical safeguards appropriate to the size and complexity of Diorthos's business, the nature and scope of the Processing, and the sensitivity of the Customer Data Processed in Diorthos-Controlled Systems, designed to protect Customer Data against a Security Incident. The program includes, at a minimum, the baseline controls stated in Annex B. Diorthos may improve its safeguards over time, provided the changes do not materially reduce the overall protection of Customer Data during a Subscription Term.

5.2 Tenant isolation

Each Customer's Tenant Knowledge Graph is provisioned in its own **dedicated, logically isolated tenant graph dataset**. Tenant datasets are never commingled in a shared graph; multiple tenant datasets may be hosted on shared Diorthos-operated infrastructure, and tenants may be partitioned across infrastructure instances as capacity grows (Product Schedule Section 3.2(a)). Diorthos will maintain the logical tenant-isolation controls and the multi-tenant application controls for Inkpad stated in Annex B, and will not represent tenant isolation as physical isolation.

5.3 Credential management

a. **Least-privilege methods.** Customer will provide service accounts, OAuth authorizations, API keys, or other least-privilege access methods rather than personal passwords where reasonably available (MSA Section 4.3).

b. **Customer authorization and revocation.** Customer is responsible for authorizing, managing, and revoking access to its source systems and Customer AI Accounts, including revoking credentials at exit (MSA Sections 4.3 and 14.4(c)).

c. **Diorthos protection.** Diorthos is responsible for protecting credentials stored in Diorthos-Controlled Systems, including storing them encrypted, limiting access to personnel who need it, and limiting use to the purposes approved in the Agreement.

d. **No credentials in ordinary support channels.** Neither Party will transmit passwords, API keys, or other authentication secrets through ordinary support channels (including email and chat-based support threads); the Parties will use the approved credential-exchange method identified in the Approved Third-Party Services Schedule or otherwise agreed in writing.

e. **No direct model exposure.** Where reasonably practicable, source-system credentials and secrets are used by deterministic Tools or integration components and are not included in prompts or exposed directly to an Approved Model Environment (Product Schedule Section 3.4(e)).

5.4 Customer security responsibilities

Customer is responsible for: (a) the security of Customer's source systems, networks, devices, and accounts, including the Customer AI Account and any Local Model Environment; (b) the portions of a Runtime Environment

allocated to Customer in the Runtime Responsibility Matrix, and all of a Customer-Provided Runtime except the obligations expressly assigned to Diorthos in the Order Form or Runtime Schedule; (c) assigning appropriate Governance Roles and maintaining the accuracy of its reviewer and approver mappings in the Tenant Graph Governance and Retention Schedule; (d) configuring provider retention and model-training settings for its Customer AI Account as recorded in the Order Form (Product Schedule Section 6.4(a)); (e) its Authorized Users' credentials and access hygiene; and (f) not submitting prohibited data categories, as stated in Section 9.

---

6. Remote Administrative Access

6.1 Customer-Provided Runtime

Diorthos access to a Customer-Provided Runtime is temporary and customer-approved. Diorthos personnel and contractors may access a Customer-Provided Runtime only through the remote-access method identified in the Approved Third-Party Services Schedule, for the support, installation, maintenance, or troubleshooting purpose for which Customer granted the access, and Customer may observe, limit, or terminate a session. Session recording is prohibited unless approved in advance by Customer.

6.2 Hosted Runtime

Customer authorizes Diorthos personnel and contractors bound by confidentiality obligations to maintain persistent administrative access to the Hosted Runtime as reasonably necessary to provision, secure, update, monitor, operate, troubleshoot, and support the Inkstamp Services. Diorthos will not intentionally access unrelated Customer files or use that access for an unauthorized purpose. This Runtime access is separate from Customer's own access to Inkpad and from Diorthos's administration of the Inkstamp Hosted Graph Service, which Diorthos operates as managed services (Product Schedule Section 3.2).

6.3 Access controls

For all remote administrative access under this Section 6, Diorthos will: (a) limit access to personnel and contractors who need it for the stated purpose and are bound by confidentiality obligations; (b) use the remote-access controls stated in Annex B, including named accounts where practical and MFA for administrative access where supported; and (c) log administrative access to Diorthos-Controlled Systems as part of its operational and security logging. "**Administrative Access Metadata**" means operator identity, target host, source address, authentication event, access start and end time, privilege-elevation event, associated support or change identifier, command executable or command category, exit status, and identifiers of resources changed; it excludes keystrokes, command arguments, standard input, standard output or error, terminal buffers, screen images, file contents, prompts, credentials, and Customer Data contained in a command. Logging of Administrative Access Metadata is not session recording for purposes of Section 6.1; capture of the excluded elements is.

---

7. Subprocessors

7.1 General authorization; current list

Customer provides general written authorization for Diorthos to engage the Subprocessors on the Approved Subprocessor List, and for the Hosting Partner identified in the Approved Third-Party Services Schedule, to Process Customer Data to provide the Inkstamp Services. The Approved Subprocessor List identifies, for each Subprocessor, the service provided, the categories of data it may Process, the purpose, and the processing region.

7.2 Updates and notice

Diorthos may add or replace a Subprocessor by updating the Approved Subprocessor List and giving Customer notice — by email to the notice or security contact identified in the Order Form, or through the Inkstamp Services (MSA Section 17.1) — at least thirty (30) days before the new Subprocessor Processes Customer Data. The notice will identify the Subprocessor, the service, the data categories affected, and the planned start date. Diorthos may engage a replacement Subprocessor on shorter notice where reasonably necessary to address an emergency, a Security Incident risk, or an unplanned loss of a Subprocessor, in which case Diorthos will give notice as soon as reasonably practicable and the objection process in Section 7.3 still applies. Until the objection window for an emergency engagement closes, the replacement Subprocessor may Process Customer Data only to the extent needed to address the emergency.

7.3 Objection right

Customer may object to a new or replacement Subprocessor on reasonable data-protection grounds by written

notice within the thirty (30)-day notice period (or, for an emergency engagement, within thirty (30) days after notice). Upon objection, the Parties will confer in good faith, and Diorthos may propose a reasonable alternative — including not using the objected-to Subprocessor for Customer's deployment where operationally feasible. If no resolution is reached within thirty (30) days after the objection, Customer may terminate the affected Inkstamp Services (and only those services) on written notice, and Diorthos will refund prepaid, unused recurring Fees for the terminated services. Termination under this Section is Customer's exclusive remedy for a Subprocessor objection.

7.4 Flow-down; responsibility

Diorthos will enter into a written agreement with each Subprocessor imposing data-protection obligations that are, in substance, no less protective of Customer Data than those in this DPA, to the extent applicable to the service the Subprocessor provides. Diorthos remains responsible to Customer for each Subprocessor's performance of Diorthos's obligations under this DPA.

7.5 What is not a Subprocessor

The following are not Subprocessors: (a) an AI provider under a Customer AI Account (Section 3.1(d)); (b) a Local Model Environment and any vendor Customer engages to host or operate it; (c) Customer's own vendors, source-system providers, and contractors; and (d) Diorthos's providers of general business services that do not Process Customer Data (for example, accounting or legal services). Materially different third-party services that will receive Customer Data require notice under Section 7.2 and a corresponding update to the Approved Subprocessor List or the Approved Third-Party Services Schedule before use.

---

8. Security Incidents

8.1 Notification

Diorthos will investigate suspected Security Incidents without undue delay. Diorthos will notify Customer without undue delay, and in any event within seventy-two (72) hours, after confirming a Security Incident, unless applicable law requires earlier notice; where the GDPR or UK GDPR applies to the affected Personal Data, Diorthos will notify Customer without undue delay after becoming aware of a personal data breach affecting that Personal Data. Notice will be given to the security contact identified in the Order Form (or, if none is identified, to Customer's notice address) by email, with follow-up through the channels stated in MSA Section 17.1 as appropriate.

8.2 Notice contents

The notice will describe, to the extent then known: (a) the nature of the Security Incident; (b) the affected data categories and, where identifiable, the affected records or individuals; (c) the approximate time period; (d) the affected Runtime Environment or Diorthos Cloud Service; (e) the remediation undertaken or planned; and (f) a Diorthos contact for follow-up. Diorthos will supplement the notice as material information becomes available, and is not required to delay initial notice to complete its investigation.

8.3 Incident classes and responsibility

The Parties distinguish the following classes of security event. Diorthos's notification obligation under Section 8.1 applies to every Security Incident, including classes (a) through (d) and the Customer-Provided Runtime carve-in stated in the Section 2 definition. For events in Customer-controlled or provider-controlled systems (classes (e) through (h)), Diorthos will notify Customer without undue delay if Diorthos becomes aware of the event, and will reasonably assist under Section 8.4, but the event is not a Diorthos Security Incident and Customer (or its provider) is responsible for investigation and legal notifications.

Class	Event	Responsibility
(a)	**Diorthos Cloud Services incident** — compromise of the Inkstamp Hosted Graph Service, Inkpad, or a tenant graph dataset	Diorthos; Section 8.1 notice applies
(b)	**Hosting Partner infrastructure incident** — compromise of Subprocessor infrastructure underlying the Diorthos Cloud Services or a Hosted Runtime	Diorthos (as to Customer), through its Subprocessor responsibility under Section 7.4; Section 8.1 notice applies
(c)	**Hosted Runtime incident (Diorthos-managed portions)** — compromise of the portions of a Hosted Runtime allocated to Diorthos or the Hosting Partner in the	Diorthos; Section 8.1 notice applies

	Runtime Responsibility Matrix	
(d)	**Diorthos internal-systems incident** — compromise of Diorthos's internal business or development systems storing Customer Data or Customer credentials, or of Diorthos-controlled credential storage	Diorthos; Section 8.1 notice applies
(e)	**Hosted Runtime incident (Customer-managed portions)** — compromise arising from Customer administrative access, Customer changes, or the portions of a Hosted Runtime allocated to Customer in the Runtime Responsibility Matrix	Customer
(f)	**Customer-account incident** — compromise of Customer source systems, Customer networks or devices, Authorized User credentials on Customer's side, or a Customer-Provided Runtime (except a compromise arising from Diorthos's remote access or personnel, which is a Security Incident under Section 2)	Customer
(g)	**Customer-admin change** — an exposure caused by an action of a Customer administrator or Authorized User acting within Customer-controlled settings	Customer; not a Security Incident
(h)	**AI-provider or Local Model Environment incident** — compromise of a Customer AI Account, the AI provider's systems, or a Local Model Environment	Customer, under its provider arrangement (MSA Sections 4.4 and 10.5)
(i)	**Unsuccessful attempts** — events excluded from the Security Incident definition in Section 2	Neither Party owes notice under this DPA

8.4 Remediation and cooperation

For a Security Incident, Diorthos will: (a) investigate and take reasonable steps to contain and remediate the incident and mitigate its effects; (b) reasonably cooperate with Customer's own investigation and compliance obligations, including providing the information described in Section 8.2 as it becomes available; and (c) preserve relevant records consistent with Section 12.6. Diorthos's obligations under this Section apply to Security Incidents; assistance with events in classes (e) through (h) of Section 8.3 beyond making relevant Diorthos logs and information reasonably available may be provided as Professional Services, except that cooperation concerning a compromise arising from Diorthos's remote access or personnel (Section 2) is included at no charge.

8.5 Legal notifications; no admission

Customer is responsible for determining whether a Security Incident or other event triggers a legal obligation to notify individuals, regulators, or other third parties concerning Customer Data, and for making those notifications; Diorthos will provide the information reasonably needed for them. Except as required by law, Diorthos will not notify a regulator or affected individuals of a Security Incident involving Customer Data on Customer's behalf without Customer's prior written approval. Neither a Security Incident notice nor any assistance under this Section 8 is an admission of fault or liability by either Party. Liability for a breach of this DPA, including a Security Incident caused by that breach, is subject to MSA Section 12, including the Supercap in MSA Section 12.3.

---

9. Permitted and Prohibited Data

9.1 Permitted categories

The data categories permitted for each Data Stream — including the permitted Personal Data, the fields removed before model inference, the fields permitted to reach a Customer AI Account, the fields retained inside a Local Model Environment, the fields permitted in the Diorthos Cloud Services and the Tenant Knowledge Graph, and the provenance fields and identifiers — are identified in the applicable Data Stream Schedule. This DPA does not exclude all Personal Data: an approved use case may legitimately require limited Personal Data (for example, a support use case may require a person's name, email address, account identifier, issue details, and prior correspondence), and the Data Stream Schedule states those categories accurately.

9.2 Prohibited categories

Unless expressly authorized in an additional schedule signed or expressly approved by both Parties (which may impose additional controls), Customer will not submit to the Inkstamp Services, and the Data Stream Schedule may not authorize, the following as Data Stream content:

a. raw payment-card data (primary account numbers) or sensitive authentication data as defined under PCI-DSS;

b. bank or financial-account login credentials;

c. Social Security numbers;

d. passport or driver’s-license numbers;
e. protected health information subject to HIPAA;
f. consumer credit reports or information subject to the Fair Credit Reporting Act;
g. biometric identifiers or biometric information;
h. highly sensitive employee tax records; and
i. authentication secrets, other than integration credentials provided to Diorthos under Section 5.3 for approved connections; and
j. other data not reasonably necessary for an approved use case, which the Data Stream Schedule may not authorize.

9.3 Provenance identifiers

The Tenant Graph Governance and Retention Schedule identifies whether provenance for Customer’s tenant contains personal identifiers and how those identifiers are minimized, pseudonymized, or retained. Where practical and legally appropriate, retained provenance may minimize or pseudonymize unnecessary Personal Data while preserving the audit relationship (Section 12.4).

9.4 Unauthorized submissions

If Customer becomes aware that data in a prohibited category under Section 9.2, or a data category not identified in the applicable Data Stream Schedule, has been submitted to the Inkstamp Services, Customer will notify Diorthos without undue delay. Upon either Party identifying such a submission, the Parties will cooperate to delete, return, or quarantine the data, subject to the governed lifecycle for any committed Governed Record. Diorthos’s Processing of an unauthorized submission before it is identified is not a breach of this DPA by Diorthos, and Customer remains responsible under MSA Section 4.2 for the rights and lawful bases for the data it supplies.

---

10. Data Region

The Diorthos Cloud Services (including each tenant graph dataset), each Hosted Runtime, and Diorthos-controlled credential storage are hosted in the **United States**, unless the applicable Order Form identifies a different region for a specific service. Customer Data held in Diorthos’s other internal business and development systems is incidental (for example, support artifacts), remains subject to Section 5 and Annex B wherever Processed, and is not systematically stored outside the United States. This Section does not govern: the processing location of a Customer AI Account (which is determined by Customer’s arrangement with its AI provider); a Local Model Environment or Customer-Provided Runtime (which Customer controls); or Customer’s own systems. Remote support may be performed by Diorthos personnel and contractors accessing Diorthos-Controlled Systems from outside the hosting region, subject to the controls in Section 6.

---

11. Individual Rights Requests

a. If Diorthos receives a request from an individual to exercise a privacy right under Applicable Data Protection Laws concerning Personal Data (including access, deletion, correction, portability, or opt-out), Diorthos will not respond substantively — except to acknowledge receipt or direct the individual to Customer, where permitted by law — and will forward the request to Customer without undue delay.
b. Taking into account the nature of the Processing, Diorthos will provide reasonable assistance with Customer’s obligations to respond to individual rights requests, primarily through the features of the Inkstamp Services — including standard export (MSA Section 7.7), search and retrieval through the Inkstamp Services, correction and deletion through the governed lifecycle, and provenance reporting. Assistance beyond these features and reasonable cooperation may be provided as Professional Services.
c. Deletion requested under an individual privacy right is performed consistent with Section 12, including the retention exceptions in Section 12.5 recognized by Applicable Data Protection Laws.

---

12. Retention, Deletion, and Return

12.1 During the Subscription Term

During the Subscription Term, Customer manages Customer Data through the Inkstamp Services, including through standard export (MSA Section 7.7), the governed lifecycle for Tenant Graph Data, and the retention configuration in the Tenant Graph Governance and Retention Schedule.

12.2 Exit timeline; active-data deletion

Upon expiration or termination of an Order Form, the export and exit sequence of MSA Section 14.4 applies, and Customer may elect return of Customer Data (through the export mechanics of MSA Sections 7.7 and 14.4(b)), deletion, or both. Diorthos will delete Customer Data in Diorthos-Controlled Systems that is not subject to an agreed record-retention requirement ("**non-retained active Customer Data**") within **thirty (30) days** after the end of the export period stated in MSA Section 14.4(b). The active-data deletion period applies only to Customer Data that is not subject to an agreed record-retention requirement; it does not override the Tenant Graph Governance and Retention Schedule, a legal hold, a regulated book-of-record requirement, or a Customer-selected read-only retention service.

12.3 Backups

Customer Data in Runtime backups and Diorthos operational backups is retained until overwritten or expired through the ordinary backup cycle stated in the Runtime Schedule or the applicable backup service selection in the Order Form, and remains protected under Section 5 until deletion. Diorthos does not restore deleted Customer Data from backups except for disaster recovery or as required by law. A Customer-requested restore of a Hosted Runtime from an available snapshot under Runtime Schedule Section 9.5 is permitted and is not, by itself, a restoration of deleted Customer Data prohibited by this Section 12.3; it is a whole-VM operational-recovery mechanism only and is not a means of selectively recovering Customer Data already deleted pursuant to a valid deletion instruction or the deletion obligations of this Section 12. Where a restore performed for an operational-recovery purpose returns to service Customer Data that had been deleted under such an instruction, Diorthos will re-execute the deletion promptly after the restore is completed. Following termination of a Hosted Runtime, the Hosting Partner is obligated under its Subprocessor terms to destroy the associated provider-side data promptly following termination of the provider service; any transitional provider-side copy — including any provider data-retrieval window or post-cancellation archival copy the Hosting Partner maintains — remains protected under the Hosting Partner's Subprocessor obligations and expires no later than thirty (30) days after the effective cancellation date. Deletion of Runtime-resident Customer Data is complete upon expiry of the ordinary backup cycle and of any such transitional copy. No provider-side retention, retrieval window, or archival copy is a service to Customer, and Customer may not rely on one to recover data after termination; retrieval of Customer files is available only as stated in MSA Section 14.4(b) and Runtime Schedule Section 12.3. The scope of Runtime backup beyond the Default Restore Point stated in the Runtime Schedule is governed by the Order Form backup selection and the Runtime Schedule; this DPA does not create a backup obligation.

12.4 Record-class retention; governed destruction

Tenant Graph Data and Governed Records are retained and destroyed according to the record-class retention schedule stated in the Tenant Graph Governance and Retention Schedule, which controls record-class retention, export, archival, and governed destruction (MSA Section 2.4(b)), including the customer-specific record classes, retention periods, custody selections, and destruction authority. Ordinary deletion of operational data is distinct from governed record destruction: Committed Governed Records and their provenance are retained and destroyed according to the applicable record-class retention schedule; destruction of a Governed Record before or at the end of its retention period requires the configured human approval, and the approval and destruction event are themselves recorded as provenance to the extent required by the retention policy. Provenance may outlive the operational content it describes where the retention schedule requires it, subject to the minimization described in Section 9.3. Where Customer selects export-and-custody at exit, Diorthos may delete its retained graph copy after transfer, retention expiry, and the required approval, as stated in the Tenant Graph Governance and Retention Schedule; any Diorthos read-only retention service continues only for the period and purpose stated in the Order Form.

12.5 Privacy-law deletion; retention exceptions

Where Applicable Data Protection Laws require deletion of Personal Data, Diorthos will delete it in accordance with this Section 12, except to the extent retention is permitted or required by Applicable Data Protection Laws or by law, including for: completing a transaction or performing the Agreement; security and incident investigation; legal claims and dispute preservation; compliance with a legal obligation, including a regulated book-of-record requirement; and the internal uses those laws permit. Where a Governed Record subject to a retention requirement contains Personal Data that must be deleted, the Parties will use the minimization and pseudonymization approach in Section 9.3 to the extent it satisfies the legal requirement.

12.6 Legal hold

Either Party may preserve Customer Data as reasonably necessary for a documented legal hold, security investigation, or dispute preservation. The preserving Party will limit preservation to what the hold requires,

maintain the protections of this DPA over the preserved data, and delete it under this Section 12 when the hold ends.

12.7 Local artifacts at exit

Locally stored artifacts on a Runtime Environment — including local AI-client transcripts and session files, local-model logs and caches, Flowbot's local database and attachment store, per-run work directories, Filetray workspaces and archive trays, `.flow-state` files, internal trays and queues, temporary files, downloaded source data, locally stored credentials, logs, screenshots, support artifacts, customer-provided model weights where applicable, and local copies of graph exports or provenance — are addressed at exit through the procedures stated in the Runtime Schedule (Product Schedule Section 6.4(d)). As between the Parties: for a Customer-Provided Runtime, Customer is responsible for deleting local artifacts and verifying deletion from Customer-controlled equipment, with reasonable standard remote assistance from Diorthos (MSA Section 14.4(c)); for a Hosted Runtime, Diorthos is responsible for the portions allocated to it in the Runtime Responsibility Matrix, and termination of the Hosted Runtime after the export period and the Retention-Transition Period (as defined in MSA Section 1), together with expiry of backups and of any transitional Hosting Partner copy under Section 12.3, completes deletion of the remaining Runtime-resident artifacts.

12.8 Confirmation

Upon Customer's written request following completion of the deletion obligations in this Section 12, Diorthos will confirm in writing the deletion of non-retained active Customer Data, and will identify any Customer Data still retained under the Tenant Graph Governance and Retention Schedule, a read-only retention service, a legal hold, or a legal requirement, with the applicable retention basis. For a Hosted Runtime, the confirmation distinguishes, as applicable: deletion of active data; expiry of Runtime restore points, snapshots, and backups through the ordinary backup cycle; and expiry of any transitional Hosting Partner copy under Section 12.3, which Diorthos may evidence by reference to the Hosting Partner's contractual deletion obligations and Diorthos's service-termination records.

---

13. Assistance and Cooperation

a. Taking into account the nature of the Processing and the information available to Diorthos, Diorthos will provide reasonable assistance with Customer's obligations under Applicable Data Protection Laws concerning: data-protection assessments and impact assessments relating to Customer's use of the Inkstamp Services; prior consultations with supervisory or regulatory authorities; and inquiries from a regulator concerning Processing under the Agreement, to the extent the inquiry concerns Diorthos's Processing.

b. Diorthos will, in the first instance, satisfy this assistance through the Agreement, this DPA, the security-review materials in Section 14, and the product documentation and features of the Inkstamp Services. Assistance that requires material additional work — including bespoke assessments, extensive questionnaire campaigns beyond Section 14, or regulator-facing documentation prepared specifically for Customer — may be provided as Professional Services.

c. Each Party will reasonably cooperate with the other Party's compliance obligations under AI, privacy, and consumer-protection laws applicable to the use of the Inkstamp Services, as allocated in MSA Section 4.6.

d. Without limiting (a), Diorthos's reasonable assistance includes, to the extent required of a service provider or processor under Applicable Data Protection Laws: cooperation with Customer's cybersecurity audits and risk assessments under the CCPA and its regulations; cooperation with Customer's automated-decisionmaking-technology notices and assessments where applicable; assistance with consumer-rights fulfillment concerning Customer Data; and provision of information in Diorthos's possession, custody, or control reasonably necessary for those purposes — in each case subject to (b) and Section 14.2.

---

14. Security Reviews

14.1 Review package

Upon Customer's written request, no more than once in any twelve (12)-month period (and additionally following Diorthos's notice of a Security Incident affecting Customer, except that item (h) remains subject to the once-annually limit in MSA Section 13), Diorthos will provide a security-review package consisting of, as available: (a) an architecture overview; (b) a security-control summary aligned to Annex B; (c) a description of tenant isolation; (d) the Approved Subprocessor List; (e) a data-flow diagram for the standard deployment models; (f) a graph-governance and retention overview; (g) responses to a standard security questionnaire of reasonable length; and (h) evidence of the insurance stated in MSA Section 13. Diorthos may update the package contents over time,

provided the categories above remain covered.

14.2 Exclusions

Diorthos is not required to disclose, and the review rights in this Section 14 do not extend to: source code; another customer's data or configuration; raw vulnerability details or penetration-test exploit details; credentials; private evaluator logic or other Inkstamp Component internals; or information that would materially weaken the security of the Inkstamp Services or violate a confidentiality obligation to a third party. Review materials are Diorthos Confidential Information under MSA Section 8.

14.3 No testing without approval

Customer will not perform, and will not authorize a third party to perform, penetration testing, vulnerability scanning, load testing, or other security testing against the Diorthos Cloud Services, a Hosted Runtime, or other Diorthos-Controlled Systems without Diorthos's prior written approval, which may be conditioned on scope, timing, and method. Testing of Customer's own systems and of a Customer-Provided Runtime does not require approval, provided it does not target Diorthos-Controlled Systems.

14.4 Mandatory audit rights

Solely to the extent Applicable Data Protection Laws grant Customer or its regulator a mandatory audit or inspection right concerning Diorthos's Processing that cannot be satisfied by the materials in Section 14.1: Diorthos will permit a scoped audit of the relevant Processing, conducted remotely unless applicable law requires otherwise, no more than once in any twelve (12)-month period, on at least thirty (30) days' written notice, during business hours, by Customer or a mutually acceptable independent auditor bound by confidentiality obligations, at Customer's expense, subject to the exclusions in Section 14.2 and to Diorthos's reasonable security and scheduling requirements. Audit findings are Confidential Information of both Parties. Diorthos's reasonable time and materials in supporting an audit beyond two (2) business days per audit may be charged as Professional Services. Where Diorthos elects, with Customer's consent, to satisfy an applicable statutory audit right through a qualified independent audit, Diorthos will arrange that audit at its own expense and provide the resulting report as required by applicable law.

14.5 Additional questionnaires

Completion of customer-specific security questionnaires, portal submissions, or assessments beyond Section 14.1 may be provided as Professional Services.

---

15. International Transfers

a. Customer Data is stored and ordinarily Processed in the region stated in Section 10 (the "**Hosting Region**"). Diorthos does not direct Customer Data outside the Hosting Region, and no persistent copy of Customer Data is stored outside the Hosting Region by Diorthos or by a Subprocessor, except as expressly identified in the Approved Subprocessor List or the applicable Order Form. Diorthos and its Subprocessors may permit **transient remote access** to Customer Data from another jurisdiction solely for support, security, incident response, or legal compliance, provided the access is need-based and least-privilege, is logged, is subject to confidentiality and security controls consistent with this DPA, and is covered by any legally required transfer mechanism. The Approved Subprocessor List identifies, for each Subprocessor, both its storage and production region and the locations from which its remote support or administrative access may occur.

b. The Parties do not anticipate that this DPA governs Personal Data subject to the GDPR or UK GDPR under the standard deployment models. If Customer intends to submit Customer Data subject to the GDPR, UK GDPR, or another law requiring a cross-border transfer mechanism, the Parties will, before that data is submitted, execute the applicable transfer mechanism — including the EU Standard Contractual Clauses and/or UK International Data Transfer Addendum, with the annexes completed from Annex A, the Data Stream Schedule, and the Approved Subprocessor List — through a Negotiated Addendum.

---

16. Liability; Term; Miscellaneous

16.1 Liability

Liability arising out of or relating to this DPA, including a Security Incident, is subject to MSA Section 12, including the exclusions in MSA Section 12.1, the General Cap in MSA Section 12.2, the Supercap in MSA Section

12.3, and the Excluded Claims in MSA Section 12.4. This DPA creates no separate or additional cap.

16.2 Term; survival

This DPA takes effect when incorporated through the applicable Order Form and remains in effect, in its entirety, for as long as Diorthos Processes Customer Data under that Order Form — including during the export period, the Retention-Transition Period, any wind-down, and any read-only retention period — notwithstanding the expiration or termination of the Order Form or the MSA.

16.3 Conflict; governing law

In the event of a conflict between this DPA and another Agreement document with respect to the subjects this DPA controls, this DPA controls (MSA Section 2.4(a)), except that a signed Negotiated Addendum controls the provisions of this DPA it expressly modifies (Section 1.2; MSA Section 2.4(d)). This DPA is governed by MSA Section 16 (Governing Law; Disputes). If a provision of this DPA conflicts with a requirement of Applicable Data Protection Laws that cannot be varied by contract, the legal requirement controls to the extent of the conflict, and the Parties will cooperate in good faith to amend the affected provision.

Annex A — Processing Details

This Annex states the standing frame for the customer-specific Processing details identified in the Order Form, the Data Stream Schedule, and the Tenant Graph Governance and Retention Schedule (Section 4.2; MSA Section 9.2).

Item	Description
Subject matter	Provision of the Inkstamp Services identified in the applicable Order Form, including the Diorthos Cloud Services, Hosted Runtime services, support, and Professional Services
Duration	The Subscription Term, plus the export period, the Retention-Transition Period, any wind-down period, and any read-only retention period, as stated in Section 12 and MSA Section 14.4
Nature of Processing	Retrieval from approved sources; deterministic processing, minimization, redaction, and normalization in the Runtime Environment; transmission of approved categories to the Approved Model Environment and the Diorthos Cloud Services; storage and governance of Tenant Graph Data through the governed lifecycle; hosting; support and remote access; export; deletion and governed destruction (Product Schedule Sections 3.3 and 3.4)
Purpose	The following specific business purposes, and no others: operating the Inkstamp Services identified in the Order Form and the approved use cases identified in each Use-Case Schedule; retrieving and processing the Data Streams identified in the Data Stream Schedule; hosting and governing Tenant Graph Data and Governed Records; authentication, access administration, and Approval-Authority enforcement; security monitoring, troubleshooting, incident response, support, and maintenance; performing contracted Professional Services; export, retention, custody transfer, deletion, and governed destruction under the Agreement; and Customer-specific improvement solely within MSA Section 7.6 and Section 4.5 of this DPA — “improving” does not permit any general commercial use of identifiable Customer Data
Categories of data subjects	As identified in the applicable Data Stream Schedule; typically Customer personnel and Authorized Users, and the customers, prospects, vendors, and other individuals whose information appears in approved sources
Categories of Personal Data	The categories expressly identified in the applicable Data Stream Schedule (Section 9.1); prohibited categories under Section 9.2 are excluded unless expressly authorized in an additional schedule
Sensitive data	None expected under the standard deployment models; a prohibited category under Section 9.2 requires an additional schedule stating the additional controls, and any other sensitive-data category must be expressly identified in the applicable Data Stream Schedule
Frequency	Continuous or as configured for each Data Stream and Filetray Flow during the Subscription Term
Retention	Section 12 of this DPA; record classes and periods per the Tenant Graph Governance and Retention Schedule
Subprocessors	The Approved Subprocessor List; the Hosting Partner and applicable services per the Approved Third-Party Services Schedule
Region	Section 10 of this DPA; any service-specific region per the Order Form

---

Annex B — Baseline Security Controls

Diorthos maintains, at a minimum, the following controls for Diorthos-Controlled Systems (Section 5.1):

1. Access control. Least-privilege access; named accounts where practical; multi-factor authentication for administrative access where supported; periodic access review; prompt deprovisioning of departed personnel.

2. Encryption. Encryption in transit; encryption at rest for Diorthos-controlled storage where supported; encrypted credential storage.

3. Tenant isolation. Dedicated, logically isolated per-tenant graph datasets; multi-tenant application controls for Inkpad (Section 5.2).

4. Governance controls. Preview → approve → commit controls for Tenant Knowledge Graph changes; server-side enforcement of Approval Authority; PROV-O-compatible provenance for governed actions (Product Schedule Section 3.3).

5. Logging and monitoring. Operational and security logging for Diorthos-Controlled Systems, including administrative access logging (Section 6.3).

6. Personnel. Written confidentiality obligations for personnel and contractors (Section 4.4); security awareness appropriate to role.

7. Change control and patching. Change control for Diorthos-Controlled Systems; patching according to the Runtime Responsibility Matrix for Hosted Runtimes and Diorthos's own schedule for the Diorthos Cloud Services.

8. Incident response. A documented incident-response process supporting the obligations of Section 8.

9. Retention and destruction. Governed retention and destruction consistent with Section 12, including the governed lifecycle for Tenant Graph Data.

10. Remote access. The remote-access controls of Section 6; prohibition on credentials in ordinary support channels (Section 5.3(d)); session recording prohibited unless approved (Section 6.1).

11. License-artifact integrity. Protection of Offline License Files against unauthorized modification in Diorthos-Controlled Systems; Offline License File behavior itself is stated in Product Schedule Section 9.3.

End of Inkstamp Data Processing and Security Addendum.