

MTDT Data Processing Agreement

Version 1.1 · 25 August 2026

This Data Processing Agreement ("DPA") is incorporated into Customer's governing agreement with MTDT and forms part of the written contract for Customer's access and use of the MTDT Services (the "Agreement") between the applicable MTDT entity as set forth in the Agreement and identified in Appendix 1 ("MTDT", "we", "us" or "our") and its customer ("Customer", "you" or "your"). This DPA applies to Personal Data provided by Customer and each Data Controller in connection with your use of the Services. All capitalized terms not defined herein have the meaning set forth in the Agreement.

1. Scope

1.1 Purpose. This DPA governs the processing of Personal Data that MTDT carries out on Customer's behalf in providing the Services, and sets out the parties' respective obligations under Data Protection Law in respect of that processing.

1.2 Governance. Customer will bind any other Data Controller it permits to use the Services to the terms of this DPA and will be solely responsible for administration of all approvals, consents, instructions or requests from other Data Controllers. Customer agrees that it shall be MTDT's sole point of contact and shall accept all information and notices on behalf of its other Data Controllers, and is solely responsible for distributing them.

2. Roles and Responsibilities

2.1 Roles. MTDT shall be Data Processor and Customer and those entities that it permits to use the Services shall be the Data Controller(s).

2.2 Responsibilities. The Appendices are incorporated into this DPA and (1) set forth the nature and purpose of processing, (2) MTDT's Technical and Organizational Measures designed to secure Personal Data, (3) MTDT's active Subprocessor list, and (4) additional obligations arising under Data Protection Law. Each party agrees to comply with its respective obligations under Data Protection Law. Customer is solely responsible for determining whether the Services meet Customer's requirements and legal obligations under Data Protection Law.

2.3 Documentation and Records of Processing. Each party is responsible for its own documentation requirements under Data Protection Law. If Customer is unable to use the functionality of the Services to obtain the information required to maintain records of processing related to Personal Data, MTDT agrees to reasonably assist Customer in obtaining such data, subject to the terms of the Agreement and technical limitations.

3. MTDT Obligations

3.1 Instructions from Customer. MTDT will follow instructions received from Customer with respect to Personal Data unless such instructions violate applicable law or require modifications to the Services. Should MTDT be unable to comply with Customer's instructions, it will notify Customer. If Union or Member State law requires MTDT to process Personal Data otherwise than as Customer has instructed,

MTDT will inform Customer of that legal requirement before it processes, unless that law prohibits it from doing so. Customer understands that a name and an email address are required to operate a user account, and that a request to delete that information may result in termination of the user account and of Customer's ability to use the Services.

3.2 Personnel. MTDT and its Subprocessors will use personnel who are informed of the confidential nature of Personal Data and of the applicable requirements of Data Protection Law, and who are bound by obligations of confidentiality.

3.3 Technical and Organizational Measures. MTDT agrees to implement the technical and organizational measures set out in Appendix 2. MTDT may modify those measures without notice to or consent from Customer if the modification does not materially decrease the overall security of the Services.

3.4 Security Breach Notification. MTDT will notify Customer without undue delay if it becomes aware of any Security Breach, and will describe the nature of the breach to the extent then known. Customer is solely responsible for its Users' access credentials and for all actions taken by its Users.

3.5 Data Subject Requests. Where Customer is able to exercise data subject rights using the functionality of the Services, Customer shall do so. Where it is not, MTDT agrees to reasonably assist Customer in responding to data subject requests in accordance with Customer's instructions and Data Protection Law, subject to the terms of the Agreement and technical limitations. If a data subject or a data protection authority contacts MTDT directly with an inquiry relating to Customer, MTDT will notify Customer and will respond only by directing the data subject or authority to Customer.

3.6 Data Protection Impact Assessment. If Customer is required by Data Protection Law to carry out a data protection impact assessment, MTDT shall provide the documents reasonably requested to demonstrate MTDT's compliance with this DPA.

4. Subprocessors

4.1 Authorized Subprocessors. Customer provides general authorization for MTDT to engage Subprocessors to fulfill its obligations under this DPA. The Subprocessors currently engaged are listed in Appendix 3, and those engaged in connection with AI-assisted features are listed in Appendix 5. At least 30 days before engaging a new Subprocessor, MTDT will inform Customer by email or by posting the update at <https://docs.mtdt.io/docs/legal-information/subprocessors>. If Customer has a legitimate objection under Data Protection Law to a new Subprocessor, Customer shall have 30 days from that notice to terminate the Agreement; if Customer does not, Customer consents to the engagement. MTDT may replace a Subprocessor without prior notice where the replacement is reasonably necessary for urgent operational or security reasons ("Emergency Replacement"), and will inform Customer without undue delay.

4.2 Subprocessor Obligations. Where MTDT engages a Subprocessor: (i) MTDT will restrict the Subprocessor's access to Personal Data to what is necessary to provide or maintain the Services and will prohibit access for any other purpose; (ii) MTDT will enter into a written agreement imposing on the Subprocessor data protection obligations equivalent to those in this DPA to the extent the Subprocessor performs the same processing; and (iii) MTDT remains responsible for its own compliance with this DPA and for the acts and omissions of the Subprocessor that cause MTDT to breach it.

5. Evidence of Compliance and Audits

5.1 Evidence of Compliance. On Customer's request, MTDT will provide the security documentation described in Appendix 2 and will complete Customer's reasonable security questionnaire, no more than once in any twelve-month period. The parties will use that documentation, together with any current third-party audit report MTDT holds, to satisfy Customer's assurance requirements before an audit under Section 5.2 is requested.

5.2 Customer Audits. Customer (or its third-party regulator, or a mutually agreeable third-party auditor) may audit MTDT's control environment and security practices relevant to Personal Data only if: (a) MTDT has not provided reasonably sufficient evidence of its compliance with the Technical and Organizational Measures in Appendix 2; (b) a Security Breach has occurred; (c) Customer or another Data Controller has reasonable grounds to suspect that MTDT is not complying with this DPA; or (d) an audit is formally requested by a data protection authority of Customer or of another Data Controller.

5.3 Audit Restrictions. An audit will be limited to once in any twelve-month period and limited in scope and timing as reasonably agreed in advance, and is subject to MTDT's security policies and procedures. An audit will be conducted as a documentary and remote review of the measures in Appendix 2; access to MTDT systems, personnel or facilities beyond that review will be granted only where the remote review does not resolve the matter that gave rise to the audit, and will not extend to any environment containing another customer's data. Each party bears its own audit expenses, except for audits under 5.2(c) and 5.2(d), where Customer bears its own expenses and the cost of MTDT's internal resources — unless the audit reveals a breach by MTDT, in which case MTDT bears its own costs and will remedy the breach at its own cost.

6. Retention, Export and Deletion

6.1 Retention. Personal Data contained in the backups, snapshots and other artifacts the Services create is retained for the retention period applicable to that artifact under the Agreement and the retention settings Customer selects in the Services, and is deleted once that period expires.

6.2 Export and Deletion. If Customer is unable to access, export or delete its Personal Data using the functionality of the Services during the term of the Agreement, MTDT shall reasonably assist Customer with a request to retrieve or delete that Personal Data in a mutually agreeable format, subject to the Agreement, Data Protection Law and technical limitations. Any data deletion obligations set out in the Agreement apply to Personal Data processed under this DPA. Personal Data may persist in MTDT's routine operational backups after deletion until those backups age out in the ordinary cycle.

6.3 Data held in Customer-controlled destinations. Where Customer configures the Services to write to a destination that Customer controls, including Customer-supplied object storage and Customer-supplied databases, MTDT does not control that destination and deletion of data written there is Customer's responsibility.

6.4 Return and Deletion on Termination. On termination or expiry of the Agreement, MTDT will, at Customer's choice, return or delete the Personal Data it processes on Customer's behalf. Customer makes that choice by written notice given no later than 30 days after termination; if Customer gives no such notice, MTDT will delete. Customer may return Personal Data to itself at any time using the export functionality of the Services, and the Agreement governs Customer's opportunity to do so before access

ends; where Customer cannot export particular Personal Data using that functionality, MTDT will provide it in a commonly used machine-readable format so far as it is reasonably able to do so. MTDT will complete deletion within 30 days of Customer's choice or, where Customer gives no notice, within 60 days of termination, unless Union or Member State law requires MTDT to store the data. Personal Data may persist in MTDT's routine operational backups after deletion until those backups age out in the ordinary cycle, and remains subject to this DPA until it is deleted.

7. International Transfers

7.1 Location of Processing. MTDT processes Personal Data in the European Union, on infrastructure operated by Hetzner Online GmbH as described in Appendix 2. MTDT does not operate a non-EU processing location for the Services, and the personnel with access to the production systems of the Services are located in the European Economic Area. MTDT is established in the United States, and the Standard Contractual Clauses therefore apply to the transfer between Customer and MTDT under Section 7.2 even though the data itself remains in the European Union. Certain Subprocessors listed in Appendix 3 and Appendix 5 process Personal Data outside the EEA; Sections 7.2 and 7.3 apply to those transfers as well.

7.2 Application of the Standard Contractual Clauses. The parties enter into and incorporate the Standard Contractual Clauses if Personal Data is transferred from the EEA, directly or by onward transfer, to a country not recognized by the European Commission as providing an adequate level of protection. To the extent the Standard Contractual Clauses apply, the terms of this DPA clarify the respective obligations within them and nothing in this DPA shall be construed to conflict with them. Module Two (controller to processor) applies where Customer is a controller of the Personal Data, and Module Three (processor to processor) applies where Customer is a processor acting on behalf of a third-party controller. The optional docking clause in Clause 7 and the optional language in Clause 11 shall not apply. Option 2 of Clause 9 shall apply, on the basis of the general authorization for subprocessors given in Section 4.1. The governing law of the Standard Contractual Clauses shall be the law of the Member State of the European Union in which Customer is established, provided that law allows for third-party beneficiary rights; where Customer is not established in a Member State of the European Union, or that law does not allow for third-party beneficiary rights, the governing law shall be the law of Poland.

7.3 Application of the UK Addendum. The parties enter into and incorporate the International Data Transfer Addendum to the Standard Contractual Clauses issued by the UK Information Commissioner (the "UK Addendum") if Personal Data is transferred from the United Kingdom to a country not covered by UK adequacy regulations or a European Commission adequacy decision. The modules in operation and the selected and optional clauses shall be the same as those reflected in Section 7.2. The "Parties' details" and the "Key Contact" shall be as stated in the Agreement. The Appendix Information in Table 3 shall be as stated in Annex I of the Standard Contractual Clauses. Both Importer and Exporter shall be checked in Table 4.

7.4 Appendices. To the extent the Standard Contractual Clauses or the UK Addendum apply, Annex I shall be deemed completed with Appendix 1 to this DPA, Annex II with Appendix 2, and Annex III with Appendix 3 and Appendix 5.

8. Liability

8.1 The Agreement's Limitations Apply. Each party's liability arising out of or relating to this DPA, whether in contract, tort or under any other theory of liability, is subject to the exclusions and limitations of liability set out in the Agreement. A claim under this DPA counts towards the aggregate liability cap in the Agreement and does not create a separate one.

8.2 What Cannot Be Limited. Nothing in this DPA or in the Agreement limits either party's liability towards a data subject or a supervisory authority where Data Protection Law does not permit that liability to be limited, including liability under Article 82 GDPR.

9. Definitions

Capitalized terms not defined herein have the meanings given to them in the Agreement.

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"Data Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

"Data Protection Law" means any applicable international, national, federal, state or local data privacy or data protection law, regulation or order, as amended from time to time, which may include without limitation Regulation (EU) 2016/679 ("EU GDPR"); the United Kingdom Data Protection Act 2018 and the EU GDPR as incorporated into UK law under the UK European Union (Withdrawal) Act 2018 ("UK GDPR"); the Swiss Federal Act on Data Protection (nFADP); the California Consumer Privacy Act as amended by the California Privacy Rights Act; and similar state-specific data protection legislation.

"Data Subject" means an identified or identifiable natural person.

"EEA" means the European Economic Area, namely the European Union Member States together with Iceland, Norway and Liechtenstein.

"Personal Data" means any information relating to a Data Subject. For the purposes of this DPA, it includes only Personal Data submitted by Customer or its Users to the Services, or which Customer instructs the Services to process on its behalf. It also includes Personal Data supplied to or accessed by MTDT or its Subprocessors in order to provide support under the Agreement.

"Security Breach" means a confirmed (1) accidental or unlawful access to or acquisition of Personal Data by an unauthorized third party, or (2) similar incident involving Personal Data for which a Data Processor is required under applicable law to notify the Data Controller.

"Services" means the MTDT software platform purchased by Customer.

"Users" means the individuals Customer authorizes to use the Services under Customer's account.

"Affiliate" means an entity that controls, is controlled by, or is under common control with a party, where control means ownership of more than 50% of the voting interests.

"Standard Contractual Clauses" means the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, or any subsequent version released by the Commission, which will automatically apply. The modules that apply are selected in Section 7.2.

"Subprocessor" means MTDt Affiliates and third parties engaged by MTDt or by MTDt's Affiliates to process Personal Data.

Signature

Accepted and agreed by the authorized representative of each party, as of the date of last signature below or, where this DPA applies by incorporation into the Agreement, as of the date the Agreement takes effect.

MTDT	CUSTOMER
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Appendix 1 — Data Processing Description

This Appendix 1 serves as Annex I to the Standard Contractual Clauses, if applicable.

Description of the Parties

The Data Exporter is the Customer that subscribed to use the Services, together with any Affiliates or Users the Customer permits to use them.

The Data Importer is MTDt, its Affiliates, and the Subprocessors listed in Appendix 3 and Appendix 5.

Subject Matter, Duration and Purpose of Processing

The subject matter of the processing is the provision of the Services. Personal Data is processed for the purpose of providing and supporting them, as set forth in the Agreement, and for as long as the Agreement is in force.

Categories of Data Subjects and Types of Personal Data

Customer may submit Personal Data of its Users to the Services. The Services require Personal Data only in the form of name and email address, for authentication, authorization and process outcome notification purposes.

The Services additionally act on Customer's instruction in respect of Customer's connected systems — Salesforce orgs, Git providers, issue trackers and databases that Customer chooses to connect — and in respect of the objects, fields, files and metadata that Customer selects. Customer determines the scope of

each such instruction and is in control of any additional Personal Data processed as a result, including the categories of Data Subjects to which it relates.

Special Categories of Data

The Services do not require special categories of Personal Data as defined in Article 9 GDPR, and MTDT does not process them for any purpose of its own. Where Customer instructs the Services to process data that includes special categories, Customer is in control of that processing and is responsible for the lawful basis for it, for the selection of objects and fields, and for configuring the masking capabilities of the Services.

Frequency and Duration of Transfer

Transfers occur on a continuous basis for as long as the Agreement is in force. Retention of Personal Data is as set out in Section 6.1 of this DPA and in the Agreement.

Contact Information of Processor

MTDT Entity	Address
Shiny Friday Deployment Club LLC EIN 35-2903596	30 N Gould St # 43289, Sheridan, WY 82801, United States

Data protection contact: mtdt@mtdt.io

Appendix 2 — Technical and Organizational Measures

This Appendix 2 serves as Annex II to the Standard Contractual Clauses, if applicable, and describes the technical and organizational measures MTDT implements and maintains under Article 32 GDPR. MTDT may adjust these measures provided the adjustment does not materially decrease the overall security of the Services during a subscription term.

The measures below are stated as mechanisms rather than as intentions. The Services are built so that the security of Customer data does not depend on organizational scale: the tenancy boundary, the handling of credentials and the authentication assurance requirement are enforced inside the platform — in the database and in the secret store — and not by operational procedure. A control enforced by the platform holds regardless of how many people operate it, and it can be inspected by Customer rather than taken on trust.

On Customer's request, MTDT will provide documentation of the architecture and controls described below, and will complete Customer's reasonable security questionnaire on the terms set out in Section 5.1 of the DPA.

I. Data Location and Hosting Infrastructure

The Services are hosted on infrastructure operated by Hetzner Online GmbH, a German company, at its facilities in Falkenstein, Germany. Personal Data processed by MTDt in the provision of the Services is stored in the European Union and is not replicated to a facility outside it.

Physical access controls, environmental controls, power redundancy and network-layer protection at the hosting facilities are provided and maintained by that operator under its own certified information security program. MTDt personnel have no physical access to the facilities.

II. Tenant Isolation and Access Control

- **Tenancy enforced in the database.** Access to Customer data is constrained by row-level security policies evaluated by the database on every query and keyed to the requesting user's team membership. The boundary therefore holds independently of the application layer: an error in application code cannot return another tenant's rows, because the query itself is filtered before it returns. Selected tables carry additional restrictive policies that must be satisfied in combination with the permissive ones.
- **Credential isolation.** Customer credentials — Salesforce access and refresh tokens, Git provider tokens, object storage keys and connected-database passwords — are held in an encrypted secret store, separate from the application data tables, and are readable only through privileged database functions that verify the caller holds the platform's privileged backend role. A compromise of an application-level session does not expose them.
- **Role-based authorization.** Permissions are evaluated per team and per functional area, and the authorization check is applied in the database rather than only in the interface.
- **Multi-factor authentication.** MFA using a time-based one-time password or an emailed one-time code is available to all Users. A team administrator can require MFA for the whole team, and the requirement is enforced through the authentication assurance level recorded on the session, which the database checks — a User below the required assurance level cannot read the team's data even with a valid session.
- **Least privilege for personnel.** Access to production systems is limited to the personnel who require it to operate and support the Services. MTDt will identify the roles holding production access on request.

III. Encryption

- Data in transit between Customer and the Services, and between the Services and Customer's connected systems, is protected with TLS.
- Customer credentials and other secrets are encrypted at rest in the secret store described in Section II.

IV. Application Security

- **Regression testing of tenancy and authorization.** MTDt maintains automated tests covering tenancy scoping and authorization behavior, together with end-to-end suites that exercise the Services against live Salesforce orgs on a scheduled basis.
- **Maintenance of the application stack.** MTDt maintains the components of the application stack and applies updates to them, giving priority to issues of higher severity.
- **Secret handling in diagnostics.** Credentials, tokens, authorization headers, JSON web tokens and private key material are masked before application logs leave the application process.

V. Logging

- Authentication events, record restores, metadata deployments, environment provisioning, health checks, static analysis runs and drift detection runs are recorded with the acting user, the object acted upon and the outcome, and are available to Customer's administrators within the Services.
- Application and infrastructure logs are aggregated in the log management service identified in Appendix 3.

VI. Business Continuity

- Customer data held in the managed storage of the Services is backed up on a routine schedule, and the hosting infrastructure provides data redundancy for system restoration.
- Where Customer configures the Services to write backups to storage that Customer controls, continuity of that storage is Customer's responsibility.

Appendix 3 — Subprocessors

This Appendix 3 serves as Annex III to the Standard Contractual Clauses, if applicable, together with Appendix 5.

Entity	Service	Personal Data involved	Location
Hetzner Online GmbH	Infrastructure hosting for the Services	All Personal Data processed in the provision of the Services	Falkenstein, Germany
Better Stack, Inc.	Aggregation of application and infrastructure logs	Operational telemetry, containing pseudonymous identifiers of users, teams and connected organizations	Log data is held in the European Union; the provider is established in the United States
Propeller Plan Sp. z o.o.	Development and technical support of the Services	All Personal Data processed in the provision of the Services, accessed as required for support and maintenance	Poznań, Poland

Entity	Service	Personal Data involved	Location
Slack Technologies	Operational alerting	Operational telemetry, as above	United States
Amazon Web Services	Delivery of transactional email to Users	Recipient email address and the content of the notification	United States
Stripe	Billing and subscription management	Email address and an MTDt-internal user identifier. Name, billing address and tax identifier, where collected, are provided by the payer directly to Stripe and are not stored by MTDt	United States

MTDT-operated services are not Subprocessors and are therefore not listed above. Services operated by MTDt that process Customer content in connection with AI-assisted features are described in Appendix 5.

Destinations that Customer selects and controls are not MTDt Subprocessors, because MTDt does not select or control them. These include object storage that Customer configures (such as Amazon S3 or Azure Blob Storage), databases that Customer configures, and the Salesforce orgs, Git providers and issue trackers that Customer connects.

Appendix 4 — California Consumer Privacy Act

1. In accordance with Sections 1798.140(j) and 1798.140(ag) of the California Consumer Privacy Act as amended by the California Privacy Rights Act (together, "CCPA"), MTDt agrees that it has not done and shall not do any of the following: a. not Sell or Share the Personal Data received from Customer; b. not retain, use or disclose Personal Data collected pursuant to the Agreement for any purpose other than performing the Services specified in the Agreement, including retaining, using or disclosing it for a Commercial Purpose other than providing those Services; c. not retain, use or disclose Personal Data collected pursuant to the Agreement outside the direct business relationship between MTDt and Customer; d. not further Collect, Sell, Share or use Personal Data collected pursuant to the Agreement without Customer's prior express written consent, and only as necessary to perform the stated business purpose; and e. not combine the Personal Data it receives from or on behalf of Customer with Personal Data it receives from or on behalf of another person, or collects from its own interaction with the Data Subject, except as permitted by the CCPA.
2. MTDt further agrees that: a. it will notify Customer in writing if it determines it cannot comply with Customer's lawful instructions for the use of Personal Data; b. on such notice, Customer is entitled to suspend the processing; c. Customer may request the information necessary to monitor and assess MTDt's compliance with this DPA and the CCPA, including information relating to independent third-party security assessments and audits, a maximum of once every twelve months or otherwise in accordance with Section 5 of this DPA; d. Customer may take reasonable and appropriate steps to validate that MTDt uses the Personal Data in a manner consistent with

- Customer's obligations under the CCPA; and e. if MTDT engages another entity to supplement the Services in a way that involves processing Personal Data, it will contract with that entity on terms compliant with the CCPA, and MTDT remains fully responsible for that entity's compliance.
3. For the purposes of this Appendix, "Commercial Purpose", "Collect", "Sell" and "Share" have the meanings given in the CCPA, and "Data Subject" and "Personal Data" include "Consumer" and "Personal Information" as used in applicable Data Protection Law.
4. To the extent similar laws of the United States require similar contract terms, this Appendix will be deemed to address those requirements to the extent permitted by law.

Appendix 5 — AI-Assisted Features

Version 1.1 · 25 August 2026

This Appendix describes the AI-assisted features of the Services, the Personal Data that may be submitted to them, and how it is processed. It is incorporated into the DPA by reference and may be updated in accordance with Section 5 of this Appendix.

1. Optional by Design

The features described here are optional. Where a feature is not enabled, no data is submitted to any AI service for that feature and the Services fall back to deterministic behavior.

2. Features and the Data Submitted

Feature	Data submitted
Deployment description summarization — generates a human-readable description of what a deployment changes	Deployment and organization identifiers, and the metadata differences of the components Customer selected

Where Customer's metadata or configuration contains Personal Data, that Personal Data may be present in the material submitted. Customer determines the organization and the scope of each request.

Output generated by these features is retained within the Services and is available to Customer.

3. How the Features Are Operated

3.1 MTDT-operated services. The features above are served by services operated by MTDT. Because MTDT operates them, they are not Subprocessors. Where such a service uses a third-party model provider on MTDT's behalf, that provider is a Subprocessor and is published in the list referred to in Section 4.

Where MTDT adds an AI-assisted feature to the Services, MTDT will describe it in this Appendix in accordance with Section 5 before Personal Data is submitted to it.

3.2 Customer-supplied model credentials. Where the Services permit Customer to supply its own model provider credentials, and Customer does so: (a) Customer designates the provider and is responsible for its own agreement with that provider, including any data processing terms; (b) that provider is not an MTD T Subprocessor, and MTD T gives no warranty as to its processing, retention or model training practices; (c) MTD T transmits to that provider only the data described in Section 2 for the feature Customer invokes; and (d) Customer's credentials are held in the encrypted secret store described in Appendix 2 Section II.

3.3 Disabling AI features. Customer may disable AI-assisted features. Where a feature is disabled, no data is submitted to any AI service for that feature.

4. AI Subprocessors

The Subprocessors currently engaged in connection with the features described in Section 2 are:

Entity	Service	Personal Data involved	Location
Google LLC	Language model inference (Gemini), used for deployment description generation	Deployment and organization identifiers, and the metadata differences of the components Customer selected, as described in Section 2 of this Appendix	United States

The current list is also published at <https://docs.mtdt.io/docs/legal-information/subprocessors>. Section 4.1 of the DPA applies to changes to it.

5. Updates to this Appendix

MTD T may update this Appendix to reflect changes to the AI-assisted feature set. MTD T will publish the current version as part of the DPA at <https://docs.mtdt.io/docs/legal-information/dpa> and will increment the version number shown at the head of this Appendix.

Where an update adds a new AI Subprocessor, or materially expands the categories of Personal Data submitted to an existing one, MTD T will notify Customer at least 30 days in advance and Customer has the objection and termination right set out in Section 4.1 of the DPA. Where an update only removes a Subprocessor, narrows the data submitted, or records a change of feature name, MTD T will publish the update without advance notice.

No update to this Appendix may reduce the obligations MTD T owes under the body of the DPA.