DATA PROCESSING ADDENDUM

(V1. 2023 NORTH AMERICA)

This Data Processing Addendum ("**DPA**"), forms part of the Terms and Conditions and Contractual Documents signed between one of the following Botify entities: Botify SAS, Botify Ltd., Botify Corp., Botify Australia Pty. Ltd, Botify Asia Pte Ltd. and Botify Japan K.K. ("**Botify**", "**Sub-processor**" or "**Service Provider**") and ("**Customer**", "**Data Controller**" or "**Business**") as set out in the signature block in the relevant Order form and is effective on the last date of signature of the relevant Order Form (" **Effective Date**").

Capitalized terms which are not defined in this DPA shall have the meaning given to them in the Agreement, however "data controller", "data processor", "data subject", "personal data", "service provider", "business" and "processing" shall have the meanings ascribed to them in the Applicable Data Protection Laws.

This DPA is entered into between Botify and the Customer to address and fulfil the obligations of the parties pursuant to: Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation** or "**GDPR**"), the California Privacy Rights Act ("**CPRA**") and any regulations promulgated thereunder, as amended from time to time if applicable, the GDPR as amended and transposed into the laws of the United Kingdom pursuant to the European Union (Withdrawal) Act 2018 and the European Union (Withdrawal Agreement) Act 2020 (the " **UK GDPR**") if applicable, and all other Applicable Data Protection Laws, and is intended to set out the conditions under which Botify shall be entitled, in the context of the Services provided in performance of the Agreement, to process personal data as directed by the Customer.

The Customer declares that all Personal Data transferred by the Customer or on the instruction of the Customer to Botify has been collected in accordance with the Applicable Data Protection Laws.

1. Scope and Applicability of this DPA

Botify provides, as defined in the Agreement, Analytics Dashboards which provide information on the structure, the crawlability and the search engines' ranking performance on the Customer's Website(s) (the "**Services**").

To provide the Services, Botify processes logs data as well as external Analytics Data from third-party tools (Google Analytics, GA 360, Google Search Console, Adobe Analytics or any other data providers a Customer wants to ingest) (the "**Analytics Data**"), on the Customer's Website, as described in the Agreement.

The logs data, IP addresses of visitors of the Customer's website ("Users") who are the subject of the Services ("**Customer Users' Personal Data**") may be communicated to Botify. Botify will act as a Data Processor or Service Provider of the Customer Users' Personal Data and Customer is the Data Controller of the Customer Users' Personal Data.

The Customer is aware that the processing of the Customer Users' Personal Data is not necessary for Botify to provide the Services, and Customer is entirely responsible for the transfer of such data to Botify.

Given the unnecessary transfer of the Customer Users' Personal Data, Botify recommends Customer anonymize such data before the logs are sent to Botify.

There is no Customer Users' Personal Data in the Analytics Data.

This DPA applies to Botify where and only to the extent that Botify processes personal data that originates from the EEA or that is otherwise subject to data protection laws and regulations applicable to the EEA, including (i) the GDPR; and (ii) the Privacy and

Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC); and in respect for the United Kingdom, any applicable national legislation that replaces or converts into domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union, including (i) the Data Protection Act 2018; and (ii) the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426), in respect of the United States of America the California Privacy Rights Act ("**CPRA**") and, any regulations promulgated thereunder, as amended from time to time (together the "**Applicable Data Protection Laws**") on behalf of Customer as a Data Processor or Service Provider in the course of providing Services pursuant to the Agreement.

2. Role of the Parties

Customer Processing of Users' Personal Data:

As the Data Controller, the Customer agrees that :

(i) it shall comply with its obligations under Applicable Data Protection Laws when processing the Customer Users' Personal Data, and more generally all personal data that it may process and communicate to Botify, and any processing instructions it issues to Botify; and

(ii) it has provided complete information and obtained (or shall obtain) all consents and rights where necessary under Applicable Data Protection Laws for Botify to process the personal data and provide the Services pursuant to the Agreement and this DPA.

As the Data Controller or a Business, the Customer is responsible for complying with its obligations under Applicable Data Protection Laws. The Customer shall indemnify and hold Botify harmless against any damages, losses, liabilities, settlements and expenses (including without limitation costs and attorneys' legal fees) in connection with any claim or action that arises from Customer's breach of this DPA or Applicable Data Protection Laws.

Botify Processing of Personal Data:
Botify shall process personal data only for the purposes described in this DPA and only in accordance with Customer's documented, lawful instructions.

The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to Botify in relation to the processing of personal data and processing outside the scope of these instructions (if any) shall require prior written agreement between the Customer and Botify.

Customer Processing of another company's data:
In the event the Customer processes personal data from another company as a Data Processor within the meaning of the Applicable Data Protection Laws, Botify acts as a subsequent sub-processor.

In this case, the Customer represents and warrants that it has given all information regarding the processing of such personal data by Botify and obtained all authorizations from the Data Controller.

If Customer processes the data of another company and communicates it to Botify, the Customer agrees to:

(i) ensure that all the necessary authorizations to enter into this DPA has been obtained from the Data Controller,

(ii) an agreement, that is fully consistent with the terms and conditions of this DPA, has been entered into with the Data Controller,

(iii) any instruction received by Botify from the Customer in execution with the Agreement are fully consistent with Data Controller 's instruction and,

(iv) all the information communicated or made available by Botify and intended for the Data Controller pursuant to this DPA are appropriately communicated to the Data Controller.

Botify shall process the Data Controller 's personal data only under Customer's instruction and not receive any instruction directly from the Data Controller when the latter is not the Customer.

3. Purposes and description of the processing

The purpose of these clauses is to define the conditions under which Botify as Data Processor is authorized to carry out, on behalf of the Customer as Data Controller, the personal data processing operations defined ("**Personal Data"**) below in Attachment A1: Purpose, Description of Processing and List of Botify's third Parties sub data Processors.

4. Commitments of Botify as Data Processor/ Service Provider

Botify shall:

- process the personal data only for the purpose of the Agreement between Botify and the Customer in the EEA or in a third country provided that the conditions of Chapter V (Transfers of personal data to third countries or international organization) of the GDPR are complied with;
- ensure that persons authorized to process the personal data are bound by a contractual or statutory duty of confidentiality;
- keep a written record of processing activities for all types of processing done on behalf of the Customer;
- Obtain the controller's general agreement to use sub-processors in accordance with Article 5 of the DPA;
- impose on its sub-processors the same data protection obligations set out in this DPA;
- at the choice of the Customer, return or delete all personal data upon completion of the processing services or on the instruction of the Customer;
- taking into account the nature of the processing, assist the Customer by appropriate technical and organizational measures insofar as possible for the fulfilment of the Customer's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III (Rights of the data subject) of the GDPR;
- Assist the controller in ensuring compliance with the obligations pursuant to Articles 35 (Data protection impact assessment) and 36 (Prior consultation) of the GDPR taking into account the nature of processing and the information available to Botify;
- make available to the Customer all information necessary to demonstrate compliance with its obligations and allow and cooperate fully with audits, including inspections, conducted by the Customer or another person authorized to this end by the Customer;
- implement and maintain appropriate technical and organizational security measures to protect personal data from security incidents and to preserve the security and confidentiality of the User's Personal Data; and
- notify the Customer without undue delay upon becoming aware of a security incident, and provide timely information relating to the security incident as it becomes known.

5. Sub-processing

Customer agrees that Botify may engage subsequent Sub-processors to process personal data on Customer's behalf. The Sub-processors currently engaged by Botify and authorized by Customer are listed in Attachment A1 to this DPA. Upon written request from the Customer, Botify undertakes to provide an updated list of the Sub-processors it has appointed. In the event of additions or changes to the list of Sub-processors, Botify shall (i) provide an updated list of its appointed Sub-processors upon written request by the Customer and (ii) provide three months' advance notice of any Sub-processors, updating this Addendum. If Botify wishes to use Sub-processors, it shall comply with the obligations regarding the transfer of personal data, and shall pass

on its own obligations to its Sub-processors. Botify is expressly authorized to freely use third party providers, without having to inform the Controller or obtain its prior approval, provided that such third-party providers do not access Users' Personal Data.

6. International Transfers of European Personal Data

Botify may transfer Personal Data from Europe outside the European Union to a country that does not provide an adequate level of protection after obtaining the Customer's prior written consent.

In this case, Botify enter into Standard Contractual Clauses ("**SCCs**") with the sub-processor and/or one of its affiliates.

The Parties acknowledge that the Applicable Data Protection Laws does not require SCCs for Customer Personal Data to be processed in or transferred to a European Union Member State or to a country subject to an adequacy decision from the European Commission pursuant to article 45 of the GDPR or, in case of a transfer from the United-Kingdom, to a country subject to an adequacy regulation from the competent United-Kingdom regulatory authority pursuant to article 45 of the UK GDPR and Section 17A of the 2018 Act (an "**Adequate Country**").

If Customer Personal Data is transferred to or processed in any country that is not an Adequate Country and if European Data Protection Law applies to the transfers (hereafter a "**EU Restricted Transfer**") or if the UK GDPR applies to the transfers (hereafter a "**UK Restricted Transfer**") (each a "**Restricted Transfer**"), the EU SCCs (Controller-to-Processor) or the UK SCCs (Controller-to-Processor) will apply with respect to such Restricted Transfers between Botify and the Customer, depending on the situation. In such a case, this DPA incorporates the relevant SCCs by reference under the conditions set out hereafter.

Nothing in the Agreement (including this DPA) is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under European Data Protection Law.

In the event that the present SCCs are invalidated, Botify and the Customer shall negotiate in good faith an acceptable alternative method to govern the transfer of data in accordance with the Applicable Data Protection Laws.

6.1 European Union SCCs:

The term EU SCCs (Controller-to-Processor) refers to the standard contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries that have been determined to provide an inadequate level of data protection., with Module 2 selected.

The Parties agree that the EU SCCs (Controller-to-Processor) will apply to EU Restricted Transfers.

Where an EU Restricted Transfer is taking place, the EU SCCs (Controller-to-Processor) will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows (where applicable):

- In Clause 7 of the EU SCCs (Controller-to-Processor), **the optional "Docking clause" will apply**;
- In Clause 9 of the EU SCCs (Controller-to-Processor), the **Option 2 "GENERAL WRITTEN AUTHORISATION" will apply**, and the time period for prior notice of any intended changes to that list through the addition or replacement of sub-processors will be **three (3) months**;
- In Clause 11 of the EU SCCs (Controller-to-Processor), **the optional language will not apply**;
- In Clause 17 of the EU SCCs (Controller-to-Processor), the **Option 1 will apply** and the SCCs will be governed by the laws of **France**;

- In Clause 18(b), dispute arising from the of the EU SCCs (Controller-to-Processor) shall be resolved by the courts of **France**;

- Annex I, Part A of the EU SCCs (Controller-to-Processor) is completed as follows:

    - Data Exporter: the Customer as defined within this DPA;

    - Data Exporter's contact information: as set forth in this DPA;

    - Data Exporter's role: Data Controller;

    - Data Exporter's Signature and Date of Signature: By entering into this DPA, the Data Exporter is deemed to have signed these Standard Contractual Clauses, which are incorporated by reference herein, including their Annexes, as of the Effective Date of this DPA;

    - Data Importer: the Botify entity signing the Agreement being either: Botify Ltd., Botify Corp., Botify Australia Pty. Ltd., Botify Asia Pte Ltd. or Botify Japan K.K.

    - Address of Data Importer:
        - Botify SAS, 7 rue d'Amsterdam, 75009, Paris, France
        - Botify Ltd., 23 Copenhagen Street, London N1 0JB, United Kingdom
        - Botify Corp., 3 World Trade Center, 49th Floor, New York, NY 10007;
        - Botify Australia Pty. Ltd. (ABN 41 652 816 610), 6 Middlemiss St Lavender Bay, Sydney NSW 2060, Australia;
        - Botify Asia Pte Ltd., 1 George St, Level 10, Singapore 049145;
        - Botify Japan K.K., c/o SU Partners Godo Gaisha Ark Hills Front Tower RoP 701, 2-23-1 Akasaka, Minato-ku Tokyo, Japan;

    - Contact person's name, position and contact details: Katia Bellon, Data Protection Officer, dpo@botify.com;

    - Signature and date of signature of the Data Importer: By entering into this DPA, the Data Importer is deemed to have signed these Standard Contractual Clauses, which are incorporated by reference herein, including their Annexes, on the Effective Date of this DPA;

- Annex I, Part B of the EU SCCs (Controller-to-Processor) shall be completed in accordance with the Attachment A1 of this DPA as follows:

    - "*Categories of data subjects whose personal data is transferred*" is completed in accordance with **article 4 of Attachment A1 of this DPA;**

    - "*Categories of personal data transferred*" is completed in accordance with **article 5 of Attachment A1 of this DPA;**

- "*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures*" is **not applicable**;

- "*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)*" is completed in accordance with **article 2 of Attachment A1 of this DPA;**

- "*Nature of the processing*" is completed in accordance with **article 6 of Attachment A1 of this DPA;**

- "*Purpose(s) of the data transfer and further processing*" is completed in accordance with **article 1 of Attachment A1 of this DPA**

- *"The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period"* is completed in accordance with the information mentioned in the table in **article 7 of Attachment A1 of this DPA;**

- *"For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing"* is completed in accordance **with article 3 and 6 of Attachment A1 of this DPA**;

- In Annex I, Part C of the EU SCCs ("Controller-to-Processor), the CNIL (https://www.cnil.fr/) is designated as the competent supervisory authority;

- Attachment A2 of this DPA will serve as the Annex II of the EU SCCs (Controller-to-Processor);

- Annex III of the EU SCCs is completed in accordance with the table in **article 7 of Attachment A1 of this DPA.**

6.2 United Kingdom SCCs

Section 1

The parties agree that the UK SCCs (Controller to Processor) shall apply to UK Restricted Transfers.

In the case of a Restricted Transfer to the UK, the UK SCCs (Controller to Processor) shall be deemed to be entered into (and incorporated into this DPA by reference).

The term UK SCCs (Controller-to-Processor) refers to the EU SCCs (Controller-to-Processor) as defined in the present DPA, completed by the International Data Transfer Addendum (the "**Addendum**") issued by the Commissioner Section 119A of the Data Protection Act 2018 which came into force on 21 March 2022. The parties agree that the UK SCCs (Controller-to-Processor) will apply to UK Restricted Transfers. Where a UK Restricted Transfer is taking place, the UK SCCs (Controller-to-Processor) will be deemed entered into (and incorporated into this DPA by this reference). With respect to Personal Data protected by the UK GDPR, the EU SCCs, supplemented as provided in Article 6 of this DPA, apply to transfers of such Personal Data, except where:

(i) The EU SCCs are deemed amended as specified by the UK Addendum, which is deemed executed between the transferring Customer (or the relevant member of the Customer Group) and Botify ;

(ii) Any conflict between the terms of the EU SCCs and the UK Addendum shall be resolved in accordance with section 10 and section 11 of the UK Addendum;

(iii) for the purposes of the UK Addendum, Tables 1 to 3 of Part 1 of the UK Addendum are deemed to be completed using the information contained in the article 6.2 of this DPA; and

(iv) Table 4 of Part 1 of the UK Addendum is deemed to be completed by selecting "no party".

Section 2

The Parties agree to be bound by the UK Addendum. In relation to any Restricted Transfer in the United Kingdom to which it applies, where the context permits and requires, any reference in the DPA to the CCAPs shall be construed as a reference to those CCAPs as amended in the manner set out in this Section 2.

7. Additional Provisions for California Personal Information

Scope. This 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information.

Roles of the Parties. When processing California Personal Information in accordance with Customer Instructions, the parties acknowledge and agree that Customer is a Business and Botify act as a Service Provider for the purposes of, and as defined in the California Privacy Rights Act ("**CPRA**") .

Responsibilities. The Parties agree that we will process California Personal Information as a Service Provider strictly for the purpose of performing the Services and any related other services under the Agreement or as otherwise permitted by the CPRA, including as described in Botify Privacy Policy.

8. List of sub-attachments:

- Attachment A1: Purposes, Description of Processing and List of Botify's Sub-processors
- Attachment A2: Technical and organizational security measures

Attachment A1
Purposes, Description of Processing and List of Botify's Sub-processors

Processing description

1. Purposes of the Processing

The main purpose of the processing of the Customer's data is the anonymization of IP Logs prior to the execution of the Service.

It is specified that Botify may process Customer data for the following additional legitimate business purposes:
(a) Hosting, storage, and processing necessary for business continuity and recovery, including the creation of backups and archives of Personal Data;
(b) System and network administration and security, including infrastructure control, identity and credential management, verification and authentication, and access control;
(c) The management and execution of Botify's internal business process leading to the indirect Processing of Customer Data for the purpose of:

- Internal audit and consolidated reporting;
- Legal compliance, including mandatory filings, uses and disclosures of information required by Applicable Data Protection Laws;
- Data anonymization and aggregation of anonymized data to enable data minimization and service analyses;
- The use of anonymized and aggregated data, as permitted by Customers, to facilitate the analysis, continuity and improvement of Botify's products and services
- The facilitation of corporate governance, including mergers, acquisitions, divestitures, and joint ventures.

2. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Customer Users' Personal Data may be transferred to the Data Importer from time to time, as needed to ensure the correct provision of the Service, under the Agreement and this DPA.

3. Duration of Treatment

The duration of the Processing is the duration of the Contract.

4. Categories of data subjects

The users of the Customer's website

5. Categories of personal data processed

Connection data (IP address, logs...)

6. Nature of the processing operations carried out by the Sub-processor on behalf of the Controller:

The processing of Personal Data carried out by the Processor consists in the consultation of Personal Data in the context of the performance of the Services under the Contract or any other agreement between the Parties.

7. List of sub-processors:

Approved Sub-processors

The controller has authorized the use of the following sub-processors:

Service/Sub-processors	Location	Function	Data Retention Duration	Type of warranty (if outside EU)
Botify UK Ltd (when acting as a subsidiary)	United Kingdom	Optional support	https://www.botify.com/data-retention-policy	DPA
Botify SAS (when acting as a subsidiary)	France	Optional support	https://www.botify.com/data-retention-policy	DPA and intra-group SCC
Botify Corp. (when acting as a subsidiary)	US	Optional support	https://www.botify.com/data-retention-policy	DPA and intra-group SCC
Botify Australia Pty. Ltd. (when acting as a subsidiary)	Australia	Optional support	https://www.botify.com/data-retention-policy	DPA and intra-group SCC
Botify Japan K.K. (when acting as a subsidiary)	Japan	Optional support	https://www.botify.com/data-retention-policy	DPA and intra-group SCC

**OVH (OVH Groupe SAS)	France, EU	Hosting	21 days*	DPA
AWS (Amazon Web Services, Inc.)	Ireland, EU	Back-up	6 months of archiving*	DPA
***AWS (Amazon Web Services, Inc.)	Germany, EU	Hosting	One-off processing, 15 days then deleted	DPA
***AWS (Amazon Web Services, Inc.)	US	Hosting	One-off processing, 15 days then deleted	DPA SCC
****Cloudflare Inc.	US	Hosting	One-off processing, 15 days then deleted	DPA SCC

**Storage and backup durations are default durations, defined to ease reprocessing if need be. All storage durations can be shortened up to a minimum of 14 days at customer request.*

***There are two ways by which Botify may obtain Data Controller data ("Transfer Method"): (a) via FTPS or SFTP transfer, or Botify pulling such data, from Data Controller's systems ("Direct"); and (b) Data Controller sending such data to Botify 's AWS S3 system ("Indirect"). OVH is only used for the "Direct" Transfer Method and AWS is always used regardless of the Transfer Method used.*

****Data from the United States may be processed in the United States and/or the European Union, unless specifically requested in the applicable Order Form. Data originating from a Customer entity located in the European Union will only be processed in the European Union.*

*****This outsourcing is only applicable when the Customer chooses the Botify PageWorkers solution.*

Note: Data from countries that have been subject to an adequacy decision by the European Commission pursuant to Article 45 of the GDPR are processed in the same way as data from the European Union.

Attachment A2

Technical and Organizational Security Measures

As a Data Processor acting on behalf of our customers, the Data Controllers, we commit to implement and maintain robust security processes and procedures.

This document summarizes the measures, both technical and organizational, that are taken for the purpose of securing and protecting data shared by our customers.

A. Controls Related to Access to Premises

Requirements	Measures
Identify authorized persons (employees and non- employees)	A list of authorized personnel is maintained
Authorization IDs	All employees have a personal badge to access to offices Access is controlled based on the user's identity.
Office/facility key access regulation	Employees are provided with electronic keys that are retrieved as part of the HR off-boarding process in case of an employee leaving the company. Lost keys are deactivated.
Non-employee access regulation	Visitors are accompanied at all times and have limited access to facilities.
Visitor logs	Visitors are required to sign-in at the facility/office's reception desk registry.
Visitor IDs	All visitors can only access the office/facility if announced and registered by a staff member and are required to provide proof of identity.
Security measures and building security	Buildings are closed outside of office hours and electronic keys are required to gain access. Entrances are monitored by CCTV. Night patrols are provided by a contracted security firm.

B. Controls Related to Data Center Locations

Requirements	Measures
Controlled access to third-party data hosting facilities	The access to third-party data hosting facilities is controlled based on the user's identity. All staff must be registered with the facility through a formal process.
Create security areas and limited access paths	Electronic access controls restrict movement within specific areas of the building only. All points of passage between areas are controlled.
Secured entrance for delivery and pick-up	Delivery and pick-up can be done in reception areas only during office hours
Secured door (electric closing mechanism, CCTV monitor)	Doors have electronic locks. Facilities are CCTV-monitored
Installation of access control features	Office buildings and data storage facilities are protected using keys, biometric devices, badge readers and man traps.
Dual monitoring	Data hosting centers have access controls in place to enter the server areas.
Measures designed to protect the premises (burglary alarm system, monitoring)	Office buildings and data storage facilities are protected with access controls: keys, badge readers, biometric gates.

C. Controls Related to Information Systems Access

Requirements	Measures
Data access terminals can be locked	Workstations, laptops and mobile devices are automatically locked when idle
Identification of a terminal and/or a terminal user for the IT system	User access to IT systems requires valid credentials. Multi-Factor Authentication is enabled when required
Roles Based Access Control	User entitlements for all accounts are managed by assigned profiles based on role and business need for access
Privacy and confidentiality obligation	Data is only accessed if customer logs support a ticket requesting help that requires accessing data. Personal Data is deleted or anonymized if received directly from Customer and only otherwise accessed if Customer requests. Contractual confidentiality agreements are executed as needed
Guidelines for document classification	Internal policies cover the classification of files and documents by level of sensitivity
Logging of data access	Data access is traceable through monitoring tools.
Inspection and control systems	Audit and logging tools track system use. Servers, networks, and software components are monitored.
Change management	The IT governance process manages change control of code and infrastructure.

D. Controls Related to Data Access

Requirements	Measures
Encryption	Encryption is enabled when required Database encryption keys are stored encrypted on separate storage
Workstation access control	Login credentials are required to gain access to any system. Multi-Factor Authentication is enabled when required
Single Sign-On authentication control	Single Sign-On is implemented to enforce centralized authentication across all of our platforms. Exceptions are documented and tracked to ensure proper off-boarding process.
Time limit of access options	Session timeouts are enabled for all software. Idle sessions are automatically terminated.
Partial access options for data inventory	Roles Based Access Controls are employed Inventory and review functions have read-only access to metadata and no access to data

E. Controls Related to Data Transmission

Requirements	Measures
Data encryption at rest and in motion.	End-to-end TLS encryption between application components. encryption of drives and media, encryption of data integration files when required. Acceptable encryption is documented in an ad-hoc policy.
Confirmation of authorized persons	Secured transfer channels, authentication by certificate and/or credentials.
Control of data carriers.	Carrying/shipping services limited to authorized providers with accompanying documents (e.g., order form, transport manifest, etc.). No physical transport of media containing Customer Data allowed.
Data carrier regulations	No physical transport of media containing Customer Data.
Controlled destruction of data carriers (e.g., misprints)	Hard copies of customer information are very limited. Persistent documents are locked away. Unnecessary paper copies are shredded and collected for disposal.
Manage production of copies	Backup copying follows a pre-defined process.
Documented data streams	All data transmission is identified and documented.
Delivery of data	No physical transport of media containing customer data
Data Integrity Check	performed at validation server level and after transit.

F. Controls Related to Inputs

Requirements	Measures
Proof of responsibilities for the data entry	Documented processes for assigning system roles and use privileges configuration
Logging of entries	Access is logged.
Program and workflow organization	Processes and responsibilities are defined in advance and assigned by roles and privileges.
Data confidentiality obligation	Employees sign contracts recording data confidentiality obligations

G. Controls Related to Availability

Requirements	Measures
Business continuity plan	Policies exist and are reviewed annually
Disaster recovery plan	Policies exist and are reviewed annually

H. Controls Related to Data Segregation

Requirements	Measures
Separation of Customers	Each customer has its own set of separated databases
Separation of functions	Each customer account manager has a specific set of customers assigned
Separation of functions	Employees belong to separate teams and execute separate functions