Data Processing Agreement

v. October 2025

BY SIGNING THIS DATA PROCESSING AGREEMENT ON BEHALF OF THE CUSTOMER, THE UNDERSIGNED REPRESENTS AND WARRANTS THAT: (A) THEY HAVE FULL LEGAL AUTHORITY TO BIND THE CUSTOMER TO THIS DATA PROCESSING AGREEMENT; (B) THEY HAVE READ AND UNDERSTOOD THE TERMS OF THIS DATA PROCESSING AGREEMENT; AND (C) THEY AGREE, ON BEHALF OF THE CUSTOMER, TO BE BOUND BY THE TERMS OF THIS DATA PROCESSING AGREEMENT.

1. Parties

This Data Processing Agreement (hereinafter referred to as the 'DPA') is entered into by and between:

Data Controller or 'Customer'	Data Processor or 'Siteimprove '
Full name of organisation:	**Full name of organisation:** Siteimprove, Inc.
Address:	**Address:** 5600 West 83rd Street, Suite 500, Bloomington, MN 55437, USA
Company registration number:	**Company registration number:** 2799877

2. Definitions

In addition to the concepts defined in the text for the DPA, these definitions shall, regardless of whether they are used in the plural or singular, in definite or indefinite form, have the following meaning when entered with capital letters as the initial letter.

'Controller' means a 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 and for the purposes of this DPA means Customer. The term 'Controller' shall also include the definition of 'Business' as set forth under the CCPA where applicable.

'Data Protection Laws' means all applicable worldwide legislation relating to data protection and privacy which applies to the Processing of Personal Data under the MSA, including without limitation: i) the General Data Protection Regulation (GDPR)[1], ii) the California Consumer Privacy Act of 2018 (CCPA)[2], iii) the UK GDPR and the Data Protection Act 2018, and iv) the new Federal Act on Data Protection (nLPD) 2020. These laws are subject to amendments, repeal, consolidation, or replacement, and any such changes will automatically be incorporated into the Processing of Personal Data under the MSA, ensuring continued compliance with applicable legal requirements.

'Data Subject' means a natural person whose Personal Data is Processed. Where applicable, this term also encompasses the definition of 'Consumer' as set forth in the CCPA.

'Data Transfer' means the transfer of Personal Data to a Third Country.

'Instruction' means the written instructions that more specifically define the object, duration, type and purpose of Personal Data, as well as the categories of Data Subjects and special requirements that apply to the Processing. Such instructions are set out in and further described in this DPA.

'Personal Data' means any information relating to an identified or identifiable natural person, where an identifiable natural person is a person who directly or indirectly can be identified in particular by reference to an identifier such as name, social security number, location data or online identifiers or one or more factors which are specific to the natural person's physical, physiological, genetic, psychological, economic, cultural or social identity. The term 'Personal Data' also encompasses 'Personal Information' as defined under the CCPA.

'Personal Data Breach' means breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed under this DPA.

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

---

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

2. California Consumer Privacy Act of 2018 (CCPA), codified as Cal. Civ. Code §§ 1798.100 et seq, as amended by the California Privacy Rights Act of 2020.

'Processor' means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller and for the purposes of this DPA means Siteimprove. The term 'Processor' shall also include 'Service Provider' as defined under the CCPA. Similarly, the Processor's Sub-Processor shall be understood as a Service Provider in the context of the CCPA.

"Processor-to-Controller Clauses" means the Standard Contractual Clauses between Processors and Controllers for Data Transfers, as approved by the European Commission Implementing Decision 2021/914 of 4 June 2021.

'Standard Contractual Clauses' means the pre-approved contractual clauses for data transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

'Sub-processor' means a natural or legal person, public authority, agency or other body which, in the capacity of subcontractor to the Processor, Processes Personal Data on behalf of the Controller.

'Third Country' means a country that is outside the European Union (EU), the European Economic Area (EEA), the United Kingdom or Switzerland and not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

3. General terms

a. Through this DPA the Customer regulates Siteimprove's Processing of Personal Data on behalf of the Customer. The aim of the DPA is to safeguard the freedoms and rights of the Data Subject during Processing, in accordance with the Data Protection Laws.

b. Siteimprove must Process Personal Data in accordance with good industry practice and follow principles and recommendations set forth in ISO 27001.

c. Two appendices are attached to the DPA and form an integral part of the DPA.

- **Appendix 1 – Instructions for the Processing of Personal Data**
  - **A - Information about the processing**
    Contains details about the Processing of Personal Data, including the purpose and nature of the Processing, type of Personal Data, categories of data subject and duration of the Processing.
  - **B – Information Security Measures**
    Contains the description of Security Measures implemented by Siteimprove.
- **Appendix 2 – Sub-processors**
  Contains the list of Sub-processors used to deliver the Software Services.

d. This DPA, which incorporates the Standard Contractual Clauses by reference, is supplemental to, and forms an integral part of, the Master Subscription Agreement (referred to as the 'MSA' in this DPA) and is effective upon its incorporation into the MSA, which may be specified in the MSA, a Service Order or an executed amendment to the MSA. In case of any conflict or inconsistency with the terms of the MSA, this DPA will take precedence over the terms of the MSA to the extent of such conflict or inconsistency. Terms not

otherwise defined in this DPA will have the meaning as set forth in the MSA. In the event of any discrepancies between this DPA and the Standard Contractual Clauses, the latter shall prevail.

4. The Customer's responsibilities

a. The Customer has the responsibility to make decisions about the purposes and means of the Processing of Personal Data. The Customer shall therefore also be responsible, among other, for ensuring there is a lawful basis for the Processing at all times and that the Instructions provided to Siteimprove (see Appendix 1) are in accordance with applicable Data Protection Laws.

b. The Customer shall, without undue delay, notify Siteimprove of any changes in the Processing which affect Siteimprove ’s responsibilities pursuant to applicable Data Protection Laws.

c. The Customer is responsible for ensuring that the Personal Data that the Customer instructs Siteimprove to process may be processed by Siteimprove, including that no special category of Personal Data (sensitive Personal Data) is made available on the Customer’s website or submitted through any other means, unless explicitly agreed upon in writing by the parties.

d. The Customer is responsible for informing Data Subjects about the Processing and protecting the rights of Data Subjects according to Data Protection Laws as well as taking any other action mandatory to the Customer according to Data Protection Laws.

5. Siteimprove 's responsibilities

a. Siteimprove undertakes to only Process received Personal Data in accordance with this DPA and for the specific purposes stipulated in the Instructions, as well as Processing Personal Data in compliance with Data Protection Laws.

b. In the event that Siteimprove finds the Instructions to be unclear, in violation of Data Protection Laws or non-existent, and Siteimprove is of the opinion that new or supplementary Instructions are necessary in order to fulfil its undertakings, Siteimprove shall inform the Customer of this without undue delay.

c. If the Customer provides Siteimprove with new or revised Instructions, Siteimprove shall without undue delay from receipt, communicate to the Customer whether the implementation of the new Instructions causes changed costs for Siteimprove.

d. Siteimprove undertakes to ensure that all natural persons working under its management follow this DPA and Instructions and that such natural persons are informed of requirements in relevant legislation.

e. Siteimprove shall, at the request of the Customer, assist with responding to requests for the exercise of a Data Subject's rights , taking into account the type of Processing and the information which Siteimprove has access to.

f. Siteimprove assures to provide sufficient expertise, reliability, and resources to assist Customer in implementing the appropriate technical and organizational measures, so that the Processing meets the requirements of the Data Protection Laws and ensures the protection of the Data Subject’s rights.

6. Security of processing

a. Siteimprove must implement appropriate technical and organizational security measures to protect Personal Data from:

   i. destruction, loss, alteration, or impairment,

   ii. disclosure to unauthorized parties or unauthorized use or from other processing in contravention of Data Protection Laws

b. At least once a year, Siteimprove must review its internal security procedures and guidelines for Processing of Personal Data to ensure that the necessary security measures are constantly observed (see Appendix 1.B)

c. Siteimprove may modify or update the Information Security Measures (Appendix 1.B) provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

7. Duty of confidentiality

a. Siteimprove must ensure that anyone who is authorized to Process Personal Data covered by the DPA, including employees and Sub-processors, undertakes a duty of confidentiality or is subject to an appropriate statutory duty of confidentiality.

b. If a Data Subject, supervisory authority or third-party requests information from Siteimprove pertaining to the Processing, Siteimprove shall inform the Customer about the matter. Information about the Processing may not be submitted to the Data Subject, supervisory authority or third parties without written consent from the Customer, unless mandatory law stipulates that such information must be provided. Siteimprove shall assist with the communication of the information covered by a consent or legal requirement.

8. Audits and inspections

a. Upon request, Siteimprove will allow for and contribute to Customer's audit by providing documentation, certifications, reports, and records relating to Processing of Personal Data for the sole purpose of determining Siteimprove 's compliance with the obligations laid down in this DPA and applicable Data Protection Laws. Customer's right to audit is limited to once per calendar year, unless there are reasonable grounds to suspect non-compliance with the DPA.

b. You acknowledge that the Software Services are hosted by our Sub-processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually and regularly tested by independent third-party penetration testing firms. Further, at your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA.

c. At Siteimprove's request, the Customer must sign a non-disclosure agreement and, in any circumstance, treat any information obtained or received from Siteimprove confidentially. The Customer or third party must not disclose such information or use such information for other purposes than to determine whether Siteimprove has taken the appropriate technical and organisational security measures.

9. Personal data breaches

a. Siteimprove must give written notice to the Customer without undue delay, after becoming aware of a Personal Data Breach.

b. Siteimprove shall, taking into account the type of Processing and the information available to Siteimprove, provide the Customer with a written description of the Personal Data Breach. Following shall be stated in Siteimprove's description to the Customer:

- the nature of the Personal Data including where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;
- the likely consequences of the Personal Data Breach;
- the measures taken or proposed to be taken by Siteimprove to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

c. If it is not possible for Siteimprove to provide the full description at the same time, according to Section 9.a of this DPA, the description may be provided in instalments without unnecessary further delay.

10. Sub-processors

a. The Customer gives Siteimprove a prior, general, written approval for the use of Sub-processors. Currently, Siteimprove is using the Sub-processors listed in Appendix 2. You may subscribe to receive notifications by email if we make changes to the Sub-processors Page by completing the form available at https://www.siteimprove.com/privacy/siteimprove-sub-processors-form/. If you opt in to receive such email, we will notify you at least 30 days prior to any such change.

b. Customer is entitled to object to the engagement of the new Sub-processor within fourteen (14) days following receipt of Siteimprove's notice. The Customer can refuse the addition or replacement of a Sub-processor if there are specific, reasonable grounds relating to the Sub-processors ability to comply with the obligations in this DPA or applicable Data Protection Laws.

c. If Customer notifies Siteimprove of such objection, the parties will discuss in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Siteimprove will, at our sole discretion, either not appoint the new Sub-processor, or permit Customer to suspend or terminate the affected Software Service in accordance with the termination provisions of the MSA without liability to either party but without prejudice to any fees incurred prior to suspension or termination.

d. Before using a Sub-processor, Siteimprove will conclude a written agreement with the Sub-processor imposing at least the same obligations as those undertaken by Siteimprove under this DPA, including the obligation to implement appropriate technical and organizational measures to ensure that the processing meets the requirements set out in the Data Protection Laws.

e. All communication between Customer and Sub-processor will take place through Siteimprove.

11. Processing location and transfer of Personal Data

a. The Standard Contractual Clauses shall apply to Data Transfers under this DPA, either directly or via onward transfer.

b. The relevant clauses for this DPA are the Processor-to-Controller clauses (Module Four), currently located **here**. The clauses are hereby incorporated by reference. The applicability of the different modules is described in the table below:

Module	When to use	Exporter	Importer
Module 1 (Controller → Controller)	Data is transferred between two controllers	Controller	Controller
Module 2 (Controller → Processor)	A controller (in EEA) transfers data to a processor (in Third country)	Controller	Processor
Module 3 (Processor → Sub-processor)	A processor (in EEA) transfers data to a sub-processor (in Third country)	Processor	Sub-processor
Module 4 (Processor → Controller)	A processor (in EEA) transfers data back to a controller (in Third country)	Processor	Controller

12. Liability in connection with the Processing of Personal Data

a. The aggregated liability of each party, including any Affiliates, arising out of or related to this DPA, will be subject to the limitations and exclusions of liability set out in the 'Limitation of Liability' Section of the MSA. Neither party's liability will be limited with respect to any compensation to natural persons suffering material or non-material damage as a result of an infringement of the applicable Data Protection Laws under this DPA.

d. Any administrative fines or similar sanctions imposed by a competent authority in relation to the Processing of Personal Data, due to an infringement of the DPA, the Instructions, and/or applicable provisions of Data Protection Laws, shall be borne by the Party to the DPA that is identified as the recipient of such sanctions.

a. If either party becomes aware of circumstances that could be damaging to the other party, the first party shall immediately inform the other party of this and work actively with the other party to prevent and minimize the damage or loss.

13. Amendments to the DPA

Unless otherwise specified, changes become effective for Customer upon renewal of the then-current Subscription Term or entry into a new Service Order after the updated version of this DPA goes into effect. Siteimprove will use reasonable efforts to notify Customer of the changes through communication via Customer's account, email, or other means.

14. Term and termination of the DPA

a. The DPA takes effect at the same time as the MSA, to which it is either annexed, incorporated by reference, or otherwise contractually linked, and will remain in effect until the termination of the MSA. Either party may terminate the DPA on the same terms and conditions as those applicable to the MSA.

b. Irrespective of the formal term of the DPA, the DPA will remain in effect for as long as Siteimprove is processing Personal Data on behalf of the Customer.

15. Measures in the event of termination of the DPA

a. Upon termination of the DPA, Siteimprove shall delete any Personal Data processed on behalf of the Customer. The obligation to delete Personal Data does not apply if storage of the Personal Data is required under EU law or relevant national law where Processing may be carried out pursuant to the DPA.

b. Deletion pertaining to the DPA shall be carried out no later than ninety (90) calendar days following the termination of the DPA, unless otherwise stated in the Instructions.

c. The Duty of Confidentiality as stated in Section 7 shall survive the termination of the DPA, and will remain in effect perpetually, or to the extent permitted by law.

16. Governing law

This DPA will be governed by and construed in accordance with the 'Governing Law' Section of the MSA, unless required otherwise by Data Protection Laws.

17. The parties signature

By signing this DPA, both parties agree to have read and understood this DPA in its entirety. The person signing represents and warrants that they are duly authorized and has the legal capacity to execute this DPA.

On behalf of Customer	On behalf of Siteimprove
Name:	**Name:**
Title:	**Title:**
Date:	**Date:**
Signature:	**Signature:**

Appendix 1 – Instructions for the Processing of Personal Data

1.A – Information about the Processing

1. Purpose and nature of Processing

The purpose of the data processor's processing of personal data on behalf of the data controller is:

a. The Customer hereby instructs Siteimprove to Process the Customer's data for use for operation and maintenance of the Customer's website, as described in the MSA. Siteimprove is a multinational software-as-a-service provider which gives customers access to cloud-based tools for management and optimization of website content, monitoring of website performance and/or use of website analysis data. The Customer has purchased access to such Software Services.

- Siteimprove's tools are designed and developed to collect and process content on Customers' websites, such as storage of cached copies of customers' website content. In this connection, Siteimprove collects and Processes both personally attributable and not personally attributable data on the Customer's website in connection with the provision of the Software Services.
- The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing): Storage of and access to personal data.

2. Type of Personal Data

a. Any Personal Data that is not considered as 'Special' (or 'Sensitive') category of Personal Data is instead categorized as 'Ordinary' Personal Data. Personal Data Processed in connection with performing the Software Services may include; name, address, e-mail address, job title, phone number or other similar non-sensitive data. Irrespective of which Software Services Customer subscribes to, only 'Ordinary' Personal Data will be Processed, unless instructed otherwise by Customer. Customer is the owner of the website (and the website content) and thereby controls what data is made available for Siteimprove to Process on Customer's behalf. Customer as Data Controller must at all times have a valid lawful basis in order to Process the Personal Data.

b. When using Analytics based services, IP addresses of website visitors may also be Processed. Siteimprove offers different technical measures to ensure irreversible anonymization of IP addresses utilized for the Analytics based services, which Customer may enable or disable at will.

c. The Processing comprises Personal Data in the categories ticked below. Siteimprove's and any Sub-processors level for security of Processing should reflect the data sensitivity.

☒ **Ordinary personal data** (see Article 6 of the GDPR)

Contact level information such as; name, e-mail address, job title, phone number

☐ **Special categories of personal data** (see Article 9 of the GDPR)

Racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, trade union membership, health issues, including abuse of medication, drugs, alcohol, etc., sexual orientation

☐ **Data on individuals' purely private affairs** (see Articles 6 and 9 of the GDPR)

Criminal convictions and offences, serious social problems, other purely private matters

☐ **National identification number** (see Article 87 of the GDPR)

3. Categories of Data Subjects

Personal Data is Processed about the following categories of Data Subjects:

- Any person who may be stated or identifiable on the Customer's website (e.g., citizens, students, employees etc.)
- Website visitors (when using Analytics based services and depending on the Customer's configuration).

4. Duration of Processing

Subject to Section 14 of this DPA, Siteimprove will Process Personal Data for the duration of the MSA, unless otherwise agreed in writing.

1.B Information Security Measures

Information security approach

Siteimprove adopts a risk-based approach to Information Security and to the protection of the Personal Data that we Process on behalf of our Customers. These measures address accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access as described in this Appendix.

The processing takes place as part of the Customers use of the Services and the Customer has the possibility to control what Personal Data is entered into the relevant Services. Siteimprove is entitled to and obliged to make decisions about which technical and organizational security measures that must be implemented in order to establish the necessary (and agreed) security level. Siteimprove will always at least take the technical and organisational measures below, but may, at any time, upgrade the level of security and the measures related thereto if the risk scenario changes.

Physical security at Siteimprove's premises and data centers	Data center physical security is managed and operated by Siteimprove's outsourced data center providers (as listed in Appendix 2). Each data center has appropriate physical security controls in place according to ISO 27001 practices. The controls in place include, but are not limited to; onsite security guards, security patrols, CCTV monitoring, and deployment of access control systems. Access to Siteimprove office locations and restricted areas is granted to authorized individuals and controlled by physical access cards. Visitors only have access to office locations when accompanied an authorized employee.
Logging	Employee activities related to Personal Data access and Processing events are logged with the following details: username, IP address, time of the activity, activity, reason for the activity. User activity logs are kept for durations dependent on the business need. Logs are kept in a centralized logging solution wherever technically feasible. Logs are inspected as part of internal security event monitoring. Monitoring processes are also independently reviewed as part of Siteimprove's ISAE 3000 and external financial audits.
Anti-malware and firewalls	Malware and endpoint protection solutions are deployed on all Siteimprove employee's devices, servers and network perimeter gateways. Procedures and responsibilities for detection, prevention and removal of malware and malicious code are implemented and communicated. Systems, devices and equipment used to access information, and systems provide host protection capabilities including anti-virus and malware detection, anomaly detection and protection and local firewalls. These are configured and managed by central policy and updated automatically. For user endpoints, Siteimprove deploys centrally managed patch management of OS, software, endpoint protection, and automatic deployment

	capabilities for applications and services. For servers, Siteimprove has the capability to rapidly patch vulnerabilities across all its computing devices, applications, and systems. Patches are assessed before being applied to production infrastructure equipment to minimize the risk of service disruption.
Incident detection and response	Siteimprove holds and maintains a Security Incident Response Plan (SIRP) based on guidelines from NIST, to address any potential data breaches or security incidents. Security incidents are detected through automated monitoring tools and manually by security teams. A reporting mechanism is available for employees to report any security vulnerabilities or suspicious activities.
Encryption	Siteimprove assures the confidentiality and integrity of Data by using and supporting the latest recommended protocols for encryption. ▪ Data in transit - When the Siteimprove platform crawls customer websites it will use the most appropriate level of TLS protocol version (e.g. TLS1.3) and cipher suites as configured by the customer's web servers, ensuring secure communication between your systems and ours. ▪ Data at rest - Siteimprove uses AES-256 encryption to protect data stored in our databases. ▪ Confidential customer data is encrypted using Transparent Data Encryption (TDE). Pseudonymization is applied, wherever feasible, by separating direct and indirect identifiers to facilitate secure and private processing. Likewise, data is logically segregated to ensure confidentiality of the information.
Backup and retention	Backup of data is completed on a regular and frequent basis. Siteimprove will store Personal Data provided by the Customer on its production environments and backups throughout the duration of the Customer's MSA with Siteimprove.
Authorization and access restrictions	The performance of Siteimprove's Software Services requires some employees to have access to the systems that process Personal Data provided by the Customer. These employees are prohibited from using their permissions to view the data unless required to carry out their defined tasks. Employee access to Data is managed in accordance with the "need to know" and "least privilege" principles, ensuring that access is granted only to those employees who require it to perform their tasks. Assignment of access privileges is aligned with the employee's current job function responsibilities. Technical controls and audit policies are in place to ensure that any access to Personal Data provided by the Customer is controlled and

	logged. Controls and policies are reviewed on a regular basis. This includes an annual review of users to ensure correct allocation of access rights. Multifactor authentication is implemented wherever technically feasible and employees' passwords are protected according to current industry best practices (NIST 800-63).
Control	**Internal security audit**: A programme of internal security audits is completed annually. The objectives of this audit programme are (i) assuring adherence to the Information Security Framework, (ii) monitoring and following-up on regulatory information security requirements relevant to Siteimprove (e.g., Personal Data processing), and (iii) indirectly raising employee awareness around Security and Privacy. **External security audit**: Siteimprove undergoes yearly security audits from third parties to obtain an objective view over the effectiveness of its technical and organizational security measures. **Penetration testing:** Siteimprove Platform is tested for security vulnerabilities through the completion of independent penetration tests and internal vulnerability assessments.

Storage period and erasure procedures

As soon as the MSA between Siteimprove and Customer is terminated, Siteimprove will initiate the deletion of Personal Data provided by the Customer. When the MSA between Siteimprove and Customer is terminated, the following will happen:

- tables in the database containing customer results, history, and specific customizations to Siteimprove platform will be dropped;
- crawled website data (HTML) and/or any linked documents (such as PDF files) will be deleted;
- deletion from backups is initiated; due to backup frequency and technical configuration, Personal Data will be fully removed from backups ninety (90) days after initiation.

User management within Siteimprove Platform

The Customer is responsible for user management within Siteimprove Platform. Access roles and rights within the Platform are predefined and detailed in the 'User Roles' section of the KnowledgeBase. There is a minimum password policy in place, but this must be configured by the Customer with more information being found on the Password Policy FAQ section of the KnowledgeBase. There is also a possibility to create additional user roles. Regarding authentication, the Platform uses its own repository of users with local authentication. It is possible to configure Single Sign On (SSO) with more information being found on the SSO FAQ section of the KnowledgeBase.

Vendor Management Process and Sub-processors

To conduct business effectively, Siteimprove collaborates with various vendors. As part of its Vendor

Management Process, Siteimprove assesses the risks tied to the products and services provided by vendors. The Vendor Management Process includes input from the Legal, Information Security, IT and Finance departments. Siteimprove's vendors are required to commit to standard provisions such as clauses regarding duty of confidentiality. Data processing agreements and other standard contractual clauses are used to further ensure secure collaborators. Siteimprove's Vendor Management Process includes regular review of vendor security measures. The frequency of review is determined by the criticality and risk rating of the vendor relationship and services.

Employee practices and information security awareness

Information security awareness training is provided as part of the new employee onboarding program which all new joiners are required to complete. Employees are made aware of security threats and practices during onboarding as well as on an ongoing basis. Employees are required to complete the mandatory annual training which includes security fundamentals, social engineering and data privacy topics. All Siteimprove employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards. Any violation of Siteimprove policies, procedures, or code of conduct may result in disciplinary actions.

Background checks: Where permitted by applicable law, Siteimprove employees undergo a third-party background or reference checks, to the extent relevant for the job and level of responsibility associated with the specific role.

Information Security Documentation

After Customer signs a non-disclosure agreement ('NDA'), Siteimprove will enable the Customer to review the following documents and information to demonstrate compliance with Siteimprove's obligations:

- the certificates issued for Siteimprove infrastructure providers in relation to the ISO 27001 Certification.
- the current SOC 2 Report for Siteimprove infrastructure providers.
- the current penetration testing attestation for Siteimprove Platform.
- the current platform architecture for Siteimprove Platform.

Security and Privacy contact

Siteimprove does not employ a Data Protection Officer, as the scale and nature of the Processing conducted by Siteimprove does not rise to the amount necessary to appoint one.

The single point of contact for Siteimprove Privacy matters is Siteimprove Privacy Team: privacy@siteimprove.com

The single point of contact for Siteimprove Security matters is Siteimprove Information Security team: security@siteimprove.com.

Customers can subscribe to status.siteimprove.com to be kept up to date with any ongoing incidents and outages. Any upcoming system maintenance updates will also be shown on this page.

Appendix 2 – Sub-processors

This Appendix constitutes Siteimprove's disclosure of Sub-processors used to provide the Software Services. It is an integrated part of the DPA, and its inclusion constitutes Customer's agreement to the use of listed Sub-processors.

In the Service Order provided by Siteimprove, under section 'Package Information', you may find a list of the relevant Software Services ordered by your organization. The table below lists all third parties used by Siteimprove to provision the Software Services.

Company name	Company Information	United States Data Centers	European Union Data Center	Processing purpose and Relevant Software Services
Amazon Web Services Inc (AWS)	**Company registration number:** 602619955 **Registered office:** 410 Terry Ave. N., Seattle, WA 98109-5210, United States	Ohio, USA	Frankfurt, Germany	**Purpose of processing:** Hosting & Infrastructure Applicable for all Customers irrespective of which Software Services you are subscribing to.
SingleStore Inc.	**Company registration number:** 3400137 **Registered office:** 534 4th St, San Francisco, CA 94107, USA	Ohio, USA	Frankfurt, Germany	**Purpose of processing:** Data Indexing Only applicable for Analytics-based Software Services.