RFP 2022-039 Annual Contract for Website Improvement Automation Product

CRITERIA	MAXIMUM SCORE	**Siteimprove, Inc. Bloomington, MN HUB - No**
Qualifications and Experience	250	191.67
Product and Implementation Requirements	450	330
Price	300	300
TOTAL SCORE	**1000**	**821.67**

Award Recommendation: Siteimprove, Inc.

Information Technology
Business First, Technology Second

Chief Information Officer
Chris Nchopa-Ayafor

Executive Assistant to CIO
Cecilia Webb

Deputy CIO
Russell Scott

Project Portfolio Management Office Director
Adepeju Ajunwon

IT Service Delivery Director
Carolyn J. Bogan

Network & Data Center Infrastructure Director
Anthony Jackson

Business Application Development & Support Director
Michael Webb

Information Security Officer
Darren May

Our vision is to be the best IT organization in state and local government within the United States.

200 Taylor Street
Fort Worth, TX 76196

Phone: 817.884.3888
Fax: 817.212.3060

www.tarrantcounty.com

3/7/22

Brad Richards
Senior Buyer
100 E. Weatherford Street, Suite 303
Fort Worth, Texas 76196

RE: RFP2022-039 – Annual Contract for Website Improvement Automation Product

Dear Mr. Richards:

Based on the information provided in the RFP responses, Tarrant County Information Technology Department approves award of RFP2022-039 to Siteimprove, Inc.

Very sincerely,

Mike Webb
Business Application Development & Support Director

Siteimprove, Inc
5600 West 83rd Street
Suite 400
Bloomington Minnesota 55437
United States

Order Form for Tarrant County
Offer Valid Through: 3/28/2022
Proposed by: George Anthony Burr
Quote Number: Q-67976.5

ORDER FORM

Address Information

Bill To:
Tarrant County
100 West Weatherford
Fort Worth Texas 76196-0401
United States

Ship To:
Tarrant County
100 West Weatherford
Fort Worth Texas 76196-0401
United States

Contact Name:
Email Address:

Phone:

Term & Payment Details

Start Date:	3/29/2022	**End Date:**	3/28/2023
Subscription Term:	12 Months	**Renewal Term:**	N/A
Subscription Term:	12 Months	**Billing Frequency:**	Annual
Payment Term:	Net 30 days	**Billing Method:**	Email
Payment Method:	Bank Transfer	**Invoice Date:**	3/29/2022
Automatic Renewal:	[ ]		

Included Services

Subscription Services	Limit Type	Quantity
Quality Assurance & Policy	Pages	15,000
Accessibility	Pages	15,000
SEO	Pages	15,000
Response	Response Check Points	3
PDF-check of documents	PDFs	30,000
Usability	Usability Maps	50

Siteimprove, Inc
5600 West 83rd Street
Suite 400
Bloomington Minnesota 55437
United States

Order Form for Tarrant County
Offer Valid Through: 3/28/2022
Proposed by: George Anthony Burr
Quote Number: Q-67976.5

Subscription Services	Limit Type	Quantity
SEO Advanced	SEO Credits	100,000
Academy Plus	Course Users	100
Elite Success Plan	N/A	1

Additional Services

Additional Services	Limit Type	Quantity	Product Price
Elite Implementation Plan	N/A	1	USD 20,000.00

Annual Subscription Fee: USD 57,517.00
Total Subscription Fee: USD 57,517.00
Additional Service Fee: USD 20,000.00

*The Order Form must be executed and/or returned to Siteimprove before the first applicable access date. If not, Siteimprove may, without changing price or term length, adjust the first applicable access date. A written acknowledgement must be received from the Customer.

Prices shown above does not include any VAT or taxes that may apply. For customers based in United States, any applicable taxes will be determined based on the laws and regulations of the taxing authority(ies) governing the Ship To Location provided by the Customer on this Order Form.

If changes are required to the Ship To Address after the contract is signed, the Customer is required to submit an Address Change Form.

When Subscription Services share the same Limit Type, the Quantity specified represents an aggregated amount, which is shared by these services.

Exceptions and Additional Terms

The Terms and Conditions of RFP 2022-039 and Siteimprove's response and exceptions to the RFP are incorporated by reference herein. In the event of a conflict between the terms of this Order Form and the Terms and Conditions of RFP 2022-039 and Siteimprove's response to the RFP including its exceptions, the terms of this Order Form shall prevail.

Sections 4(a) and 4(b) of the Terms of Use shall be removed in their entirety and replaced with the following:

a. GDPR. With respect to obligations to data subjects under the General Data Protection Regulation (EU) 2016/679 ("GDPR"), where applicable, Customer is a "data controller" and Siteimprove is a "data processor" (as such terms are defined in the GDPR). The Included Services are designed and developed to collect and process our Customers' website content and certain operational data in relation thereto. Any personal data processed by Siteimprove when performing the Included Services is processed according to the Customer's instructions and on its behalf. To fulfill both parties' obligations under the GDPR, Customer is responsible for entering into a Data Processing Agreement

("DPA") with Siteimprove which lives up to any then-current legal standards. If the use of the Included Services on Non-Public Websites and/or websites that contain special categories of personal data has been agreed upon, the Customer ensures that the DPA reflects the processing of non-public and/or special categories of personal data. If Customer has not facilitated a DPA to be signed on the day that Customer begins to use the Included Services, the parties are deemed to have entered into Siteimprove's standard DPA attached hereto.

b. CCPA. As between the parties, with respect to obligations to consumers under the California Consumer Privacy Act ("CCPA"), where applicable, Customer is a "business" and Siteimprove is a "service provider" (as such terms are defined in the CCPA) and each party will be responsible for its respective obligations under the CCPA, as applicable to the Agreement. The Included Services are designed and developed to collect and process our Customers' website content and certain operational data in relation thereto. Any personal data processed by Siteimprove when performing the Included Services is processed according to the Customer's instructions and on its behalf. The parties are deemed to have entered into Siteimprove's CCPA Data Processing Agreement, attached hereto.

Siteimprove, Inc
5600 West 83rd Street
Suite 400
Bloomington Minnesota 55437
United States

Order Form for Tarrant County
Offer Valid Through: 3/28/2022
Proposed by: George Anthony Burr
Quote Number: Q-67976.5

Purchase Order Information

(Customer to complete)

Is a Purchase Order (PO) required for the purchase or payment of the products on this Order Form?
[ ] **No**
[ ] **Yes**

Is PO renewal required for each invoicing term?
[ ] **No**
[ ] **Yes**

PO Number: _____

PO requests must be sent to: _____

Billing Information

(Customer to complete)

Billing Contact Name: _____

Billing E-mail: _____

Billing References: _____

E-invoicing Information: _____

Sales Tax Information

(Customer to complete)

You may be subject to sales tax (or equivalent) unless you can provide proof of exemption. Are you exempt from sales tax?
[ ] **Yes, please attach exemption form.**
[ ] **No.**

Siteimprove, Inc
5600 West 83rd Street
Suite 400
Bloomington Minnesota 55437
United States

Order Form for Tarrant County
Offer Valid Through: 3/28/2022
Proposed by: George Anthony Burr
Quote Number: Q-67976.5

Customer Signature

By signing below, Tarrant County agrees to the subscription and payment terms of this Order Form.

On behalf of Customer:

Name:

Date:

_____
Signature

SITEIMPROVE TERMS AND CONDITIONS

1. GENERAL TERMS

By accepting the Order Form, by paying the Annual Subscription Fee and/or Prorated Subscription Fee specified in the Order Form or otherwise making use of the Included Services, the Customer agrees to be bound by these terms of use for the Included Services, including the specifications of the Order Form (combined the "Terms"). Furthermore, any action from the Customer specifying its wish to purchase the Included Services after having received these Terms, such as sending a purchase order, shall be considered actively consenting to these Terms.

2. INVOICING

a. Invoicing Details.

All invoicing details are specified in the Order Form.

b. Failure to Pay.

Late payments may bear interest at the rate of 1% per month, or the highest rate permitted by law, whichever is lowest, from the payment due date until paid in full. Additionally, in the event that an invoice becomes overdue, Siteimprove will notify Customer by phone or email. After Siteimprove has provided notice, Customer will have five (5) business days to pay the overdue invoice. If Customer fails to make the payment by the end of the notice period, then Siteimprove reserves the right to suspend provision of the Included Services until payment has been made.

3. USE OF THE INCLUDED SERVICES

a. Ownership.

Siteimprove owns and shall remain the sole owner of all intellectual property rights vested in the Included Services created prior to or during the performance by the parties under these Terms. This ownership right includes any inventions, patents, utility model rights, copyrights, design rights, mask works, trademark rights, or knowhow, whether registered or not.

b. Right to Use.

Siteimprove grants the Customer the right to use the Included Services (the "Subscription"). The Subscription granted is worldwide, revocable, non-exclusive, non-perpetual and non-transferable. The Customer has no right to retain or to use the Included Services after termination of the Initial Subscription Term or a Renewal Term (if applicable). Customer can create an unlimited number of users to the Included Services. Customer will have access to the Included Services only for those website domain(s) specifically agreed upon with Siteimprove. This right includes updates and new releases of the Included Services, but not new modules/services/products added to the Included Services.

c. Limitations of Use.

The Customer's use of the Included Services on such website(s) is subject to the agreed quantities as specified in the Order Form (the "Limits"). If the Customer exceeds the Limits, Siteimprove will notify the Customer of such excess use and discuss appropriate upgrades of the Customer Subscription. Subject to section 9 below, Customer must be the owner or authorized administrator of the website(s) on which the Included Services are run. Unless agreed otherwise, the Included Services may not be run on any websites that contain sensitive information or special categories of personal data, e.g. as defined in the General Data Protection Regulation (EU) 2016/679 Article 9 or information subject to heightened regulations (e.g. HIPAA, FERPA). Customer has no right to rent, lease, assign, transfer, sublicense, display or otherwise distribute or make the Included Services available to any third party, unless specifically stated in section 9 (Assignability). The Included Services may not be (a) used in the performance of services for or on behalf of any third-party or as a service bureau; (b) modified, incorporated into or combined with other software, or created as a derivative work of any part of the Included Services; or (c) used for any illegal purpose. Customer may not modify, disassemble, decompile or otherwise reverse engineer the Included Services nor permit any third-party to do so except as expressly permitted by law.

d. IP Indemnification.

Siteimprove will indemnify and hold Customer harmless from all third-party claims that use of the Included Services constitutes an infringement of any third-party intellectual property right(s), unless such claim is

based on Customer's wrongful or illegitimate use of the Included Services. The foregoing states the entire liability of Siteimprove and the sole and exclusive remedy for Customer with respect to any third-party claim of infringement or misappropriation of intellectual property rights.

e. For Non-Public Website Use.

Any use of the Included Services on customer intranet, log-in-protected websites, staging websites, or any other form of non-public websites ("Non-Public Websites") is subject to the obligations set out in this Section 3(e). For Siteimprove to allow that the Included Services are used on a Non-Public Website, Customer must ensure that there is an encrypted line for the secure transport of data between Customer and Siteimprove, e.g. by ensuring all pages are served with https, or providing access through a designated VPN. Customer must ensure that, to the extent necessary, or required by applicable laws, it has an appropriate legal basis for the processing of personal data for the purpose of the Included Services, and that it has the right to disclose any confidential information on the Non-Public Website. Additionally, Customer must assign an account with non-administrative rights to the Non-Public Website when using the Included Services on any website behind log-in protection.

In the event of any failure by Customer to adhere to the obligations set out in this section, Siteimprove may reject to perform the Included Services on the Non-Public Website. Customer expressly understands and agrees that Siteimprove and its affiliates, directors and employees shall not be liable to Customer under any theory of liability for any direct, indirect, incidental, consequential or other special damages arising out of or due to Customer's use of the Included Services if such use is in breach of Customer's obligations in this section.

4. DATA & PRIVACY

a. GDPR.

With respect to obligations to data subjects under the General Data Protection Regulation (EU) 2016/679 ("GDPR"), Customer is a "data controller" and Siteimprove is a "data processor" (as such terms are defined in the GDPR). The Included Services are designed and developed to collect and process our Customers' website content and certain operational data in relation thereto. Any personal data processed by Siteimprove when performing the Included Services is processed according to the Customer's instructions and on its behalf. To fulfill both parties' obligations under the GDPR, Customer is responsible for entering into a Data Processing Agreement ("DPA") with Siteimprove which lives up to any then-current legal standards. If the use of the Included Services on Non-Public Websites and/or websites that contain special categories of personal data has been agreed upon, the Customer ensures that the DPA reflects the processing of non-public and/or special categories of personal data. If Customer has not facilitated a DPA to be signed on the day that Customer begins to use the Included Services, the parties are deemed to have entered into Siteimprove's standard DPA available at https://siteimprove.com/en/privacy/.

b. CCPA.

As between the parties, with respect to obligations to consumers under the California Consumer Privacy Act ("CCPA"), Customer is a "business" and Siteimprove is a "service provider" (as such terms are defined in the CCPA) and each party will be responsible for its respective obligations under the CCPA, as applicable to the Agreement. The Included Services are designed and developed to collect and process our Customers' website content and certain operational data in relation thereto. Any personal data processed by Siteimprove when performing the Included Services is processed according to the Customer's instructions and on its behalf. For more information on Siteimprove's Data Privacy & Security practices, including an optional CCPA Data Processing Agreement, visit https://siteimprove.com/en/privacy/.

c. Data Processing of Users and Customer Contacts.

Other than the processing of Customer's data under 4(a) and 4(b), Siteimprove collects some general usage and contact information about the users of Siteimprove's services and other contact persons provided by Customer, such as the names and emails of the Siteimprove users, for internal necessary purposes such as customer identification, invoicing, support and sharing information about Siteimprove products to Customer. A detailed description on how Siteimprove processes Customer's data under this section is available at: https://siteimprove.com/en/privacy/privacy-policy/. In this regard, Siteimprove will be the data controller under GDPR and business under CCPA and the Customer acknowledges and agrees that general customer and user

information will be collected for Siteimprove's internal use. The Customer has the right to access, correct, modify and erase any personal data provided by the Customer to Siteimprove. To exercise these rights contact privacy@siteimprove.com.

d. Customer Owned Data.

All data provided to Siteimprove through the use of the Included Services is and shall remain Customer property. Siteimprove does not resell any Customer owned data. Data mentioned under Section 4(a-b) will not be disclosed or transferred to any third-party unless otherwise specifically agreed. Data mentioned under Section 4(c) will only be disclosed or transferred to a third-party to the extent necessary to provide the Services. To enable Siteimprove to provide Customer with the Included Services, and subject to these Terms, Customer hereby grants to Siteimprove a non-exclusive right to use and process data provided by Customer solely in connection with Siteimprove's operation of the Included Services.

5. LIMITATION OF LIABILITY

Each party shall only be liable for direct damages. As such, each party shall not be liable to the other party for any indirect, special, incidental, or punitive damages caused by Customer's use of the Included Services, including, but not limited to, loss of data, loss of business or any other loss arising out of or resulting from a party's performance under these Terms, even if it has been advised of the possibility of such damages. Except where excluded by applicable law, a party's cumulative liability under these Terms shall not exceed the amount of the Fee. However, in no event shall a party be able to claim a limitation on its liability in the event of; i) non-compliance with obligations concerning personal data; ii) any third-party IP infringement claim, unless such claim is based on a party's wrongful or illegitimate use of the Included Services; or iii) gross negligence or willful misconduct.

6. REPRESENTATIONS AND WARRANTIES

a. For Siteimprove.

Siteimprove represents and warrants that: (i) it has the full power and authority to enter into and perform its obligations under these Terms; and (ii) the Included Services will perform substantially as described in these Terms for the Initial Term and any Renewal Term, provided that it is used in accordance with these Terms, including on the specified domains. These representations and warranties are only for the benefit of Customer.

b. For Customer.

Customer represents and warrants that: (i) it has the full power and authority to enter into and perform its obligations under these Terms; and (ii) it has full and legal right or authorization to display, disclose, transfer, assign or convey the information set forth and accessible on the websites on which the Included Services will be administered.

c. Disclaimer.

Except for the express representations and warranties listed in these Terms, each party makes no representations or warranties of any kind, whether express or implied. No oral or written information or advice given by either party will create a representation or warranty. Specifically, Siteimprove makes no representations or warranties with regard to the use of the Included Services for the purpose of ensuring Customer's compliance with any laws or regulations.

7. TERMINATION OF SERVICES

a. Termination of Auto-renewing Subscriptions.

During the Initial Subscription Term or any subsequent Renewal Term (if applicable), either party may cancel renewal of the Subscription for convenience by giving written notice to the other party in accordance with the specifications in the Order Form.

b. Termination with Cause.

Without affecting any other right or remedy available to it, either party may terminate the Subscription with immediate effect in the event of a material breach by the other party. Material breach shall include: (i) any violation of the terms of Articles 2(b), 3(b-e), 4(c-d), 6(a-b), 8, and 9; (ii) any other breach that a party has failed

to cure within fourteen (14) calendar days after receipt of written notice by the other party; (iii) an act of gross negligence or willful misconduct of a party; and (iv) the insolvency, liquidation or bankruptcy of a party.

c. Reimbursement.

In case of Customer termination under section 7(a) or Siteimprove termination under section 7(b), Customer remains liable for payment of all Fees owed and will not be entitled to a credit or refund. In case of termination by Siteimprove under section 7(a), Customer is entitled to a pro-rated refund corresponding to the remaining period of the Initial or Renewal Term, whichever is applicable.

8. CONFIDENTIALITY

Each of the parties agrees to (a) maintain in confidence any non-public information of the other party, whether written or otherwise, disclosed by the other party in the course of performance of these Terms ('Confidential Information'); (b) use its best endeavors to protect Confidential Information in accordance with the same degree of care with which it protects its own Confidential Information; and (c) not disclose the other party's Confidential Information to any third party, except in response to a valid order by a court or other governmental body or as required by law. The receiving party will promptly give notice to the disclosing party of any disclosure of the other party's Confidential Information.

9. ASSIGNABILITY

These Terms are binding upon and will only benefit the parties. Except as otherwise expressly provided in these Terms, neither party may assign, transfer, convey or encumber these Terms or any rights granted in them without the prior written consent of the other party (such consent not to be unreasonably withheld). Notwithstanding the foregoing, a party shall have the right to assign these Terms to its Affiliates or to a successor entity in the event of a merger, consolidation, transfer, stock purchase, provided the assignee is subject to all obligations under these Terms.

10. LAW & DISPUTE RESOLUTION

a. For Customers in Australia, EEA, Switzerland, Canada the United States.

These Terms and any dispute in relation to the Included Services, or the Customer's use hereof, will be governed by and construed in accordance with the laws of the country, state or province, whichever is applicable, where the Customer is located as specified in the Ship To address of the Order Form (the "Governing Territory"). In the event of any lawsuit or proceeding arising out of or related to these Terms, the courts of the Governing Territory will have exclusive jurisdiction.

b. For Customers in other territories.

These Terms and any dispute in relation to the Included Services, or the Customer's use hereof, will be governed by and construed in accordance with the laws of the country where the Siteimprove entity specified in the Order Form is located (the "Governing Territory"). In the event of any lawsuit or proceeding arising out of or related to these Terms, the courts of the Governing Territory will have exclusive jurisdiction.

11. RELATION TO OTHER DOCUMENTS

These Terms constitute the entire agreement between the parties and supersede any prior communications, commitments, or agreements, oral or written, with respect to the subject matter of these Terms. Any other standard or boilerplate terms and conditions included in any document provided by one party to another (e.g., click-wrap agreements and purchase orders) are not to be considered agreed upon and will not be binding on either party. Any changes or modifications to these Terms must be in writing and signed before taking effect.

Siteimprove, Inc
5600 West 83rd Street
Suite 400
Bloomington Minnesota 55437
United States

Order Form for Tarrant County
Offer Valid Through: 3/28/2022
Proposed by: George Anthony Burr
Quote Number: Q-67976.5

ELITE SUCCESS PLAN

1. Scope of Services. Siteimprove provides Elite support, education services, and advisory services as set forth in this Elite Success Plan.

2. Customer Success Manager. Elite Success Customers are assigned a Customer Success Manager (CSM) – a solution expert who understands the Customer's business priorities and desired outcomes. The CSM quickly and effectively collaborates with technical support and other Siteimprove teams to manage the Customer's issues to resolution, offers guidance to the Customer on best practices and training needs of users, and reports progress on a regular basis. During the Initial Term and each Renewal Term, the CSM will schedule quarterly strategy calls with Customer.

3. Education Services. Customer shall have access to Siteimprove's Academy Plus, Self-Help Resources, and training during the Initial Term and any Renewal Term.

3.1 Academy Plus. The Included Services include access to Siteimprove's Academy Plus for up to 20 users at no additional charge. Siteimprove's Academy offers courses on Accessibility, Analytics, and SEO (each a "Course"). Academy Plus includes all Courses and learning tracks, a team leaderboard, administrative capabilities, and reporting. Academy Plus can be accessed through your dashboard at http://my.siteimprove.com.

3.2 Self-Help Resources. Customers can take full advantage of Siteimprove self-help tools, available online via our https://support.siteimprove.com/hc/en-gb (https://support.siteimprove.com/). From that page, Customers can find links to technical documentation and knowledge base articles, discuss issues with other users in our community forums, review what's new, read technical notes, and access free webinars.

3.3 Training. Customer will receive two (2) consecutive days of training during the Initial Term and each Renewal Term with a Siteimprove employee. Customer and Siteimprove will cooperate in scheduling the training based on Siteimprove resource availability. Unused training days do not rollover from one term to another.

4. Advisory Services. Customer will receive up to ten (10) hours of Advisory Services with Siteimprove's domain experts during the Initial Term and each Renewal Term. Unless scheduled with training set forth in Section 3.3, the Advisory Services will be conducted over the phone or internet from Siteimprove's office. Customer and Siteimprove will cooperate in scheduling the Advisory Services based on Siteimprove resource availability. Siteimprove has sole discretion to determine which resources to assign to Advisory Services. Advisory Services do not include any form of remediation; Customer is solely responsible for all remediation based on the results of Advisory Services. Unused Advisory Service hours do not rollover from one term to another.

5. Product Support and Training. Customers can contact Siteimprove for product support, training, and additional services by visiting our https://support.siteimprove.com/hc/en-gb. At that location, Customers can submit a support ticket 24x7 every day of the year.

5.1 Services Levels. Siteimprove will utilize commercially reasonable efforts to promptly respond to all requests. Siteimprove aspires to review and respond to at least ninety percent (90%) of all tickets and requests within one (1) Business Day. "Business Day" is defined as one of the days on which any regional support center is open for business (see Section 6). For critical errors, meaning errors which cause the service to be down or unavailable, Siteimprove guarantees Elite Customers to work nonstop (within EMEA business hours) until such error is resolved with regular updates to the Customer. Besides general questions and technical issues, services covered by these tickets and requests include 12 hours of custom configuration (Event Tracking, Custom CMS Deeplinks, Custom Policies etc.).

6. Support and System Availability. Siteimprove has regional support centers servicing the Americas, EMEA and APAC, providing Elite Customers with global support. Siteimprove will maintain its systems and operations to

ensure Customer has access to the Included Services ninety-nine-point-nine percent (99.9%) of the time ("**System Availability**").

https://support.siteimprove.com/hc/en-gb/articles/360002402297

7. Liabilities. Siteimprove will exercise its best efforts to meet the standards set forth in this plan. In the event of a material failure to meet the above standards in any given month, a service credit in the amount of three percent (3%) of the pro-rated annual subscription fees for the applicable month will be issued for Customer and available for future subscription fees ("**Service Credit**"). Siteimprove has no obligation to issue any Service Credit unless (i) Customer reports the material failure to Siteimprove immediately on becoming aware of it; and (ii) requests such Service Credit in writing within three days of the failure. In no event will a Service Credit exceed 10% of the annual subscription fee as set forth in the Agreement. The Service Credit is non-refundable upon termination of Customer's Agreement with Siteimprove. The parties acknowledge and agree that the Service Credit is intended to be Customer's sole and exclusive remedy with respect to any failure by Siteimprove under this plan.

8. Scheduled Downtime. Siteimprove will notify Customer through email alerts at least twenty-four (24) hours in advance of all scheduled outages of the included Services ("**Scheduled Downtime**") as long as Customer has signed up for the alerts at http://status.siteimprove.com.

9. Term. This Elite Success Plan remains in force for as long as Customer continues to pay Siteimprove for the Elite Success. Siteimprove has sole discretion to update the terms of this plan at any time. In such event, said update(s) will not result in a reduction in the level of support set forth in this plan. Any updates shall be provided to Customer in a timely fashion.

Siteimprove, Inc
5600 West 83rd Street
Suite 400
Bloomington Minnesota 55437
United States

Order Form for Tarrant County
Offer Valid Through: 3/28/2022
Proposed by: George Anthony Burr
Quote Number: Q-67976.5

ELITE IMPLEMENTATION PLAN

1. Scope of Services. Siteimprove provides set-up, configuration, data integration, education services, and advisory services as set forth in this Elite Implementation Plan.

2. Implementation Team. Siteimprove will assign a Strategic Engagement Manager, Technical Support Engineer, and Implementation Analyst to Customer to manage the Elite Implementation Plan.

3. Timeline. Scope of Services described in Section 1 and this Implementation Plan shall take approximately 8-12 weeks from the Effective Date. During this time and upon completion, the Included Services can be accessed at http://my.siteimprove.com/.

4. Set-Up and Configuration. The Implementation team will work with Customer to set up and configure its account. Set-up and configuration may include the following:

- Configuration of access settings for users and groups
- 10 hours of custom configuration. Custom Configuration could include but is not limited to:
  - Advanced policies
  - Dashboards and reports
  - Behavior Maps and User Journeys
  - CMS deep-link
  - Event-tracking setup
  - Internal search tracking
- Set-up of Development website crawls (subject to additional terms and conditions)
- Set-up of non-public website (excluding development sites and subject to additional terms and conditions)
- SSO configuration and access
- API Support

5. Data Integration. The implementation team will assist Customer with data integration. This includes, but is not limited to, AEM, Jira, Tableau, or Sitecore.

6. Education Services. Customer shall have access to Siteimprove's Academy Plus and Self-Help Resources during the Initial Term and any Renewal Term.

6.1 Academy Plus. The Included Services include access to Siteimprove's Academy Plus for up to 20 users at no additional charge. Siteimprove's Academy offers courses on Accessibility, Analytics, and SEO (each a "**Course**"). Academy Plus includes all Courses and learning tracks, a team leaderboard, administrative capabilities, and reporting. Academy Plus can be accessed through your dashboard at the URL stated above.

6.2 Self-Help Resources. Customers can take full advantage of Siteimprove self-help tools, available online via our https://support.siteimprove.com/hc/en-gb (https://support.siteimprove.com/). From that page, Customers can find links to technical documentation and knowledge base articles, discuss issues with other users in our community forums, review what's new, read technical notes, and access free webinars.

7. Advisory Services. Customer will receive a one (1) day discovery and design workshop with Siteimprove. Customer and Siteimprove will cooperate in scheduling the Advisory Services based on Siteimprove resource availability.

Data Processing Agreement

67976.3

This Data Processing Agreement (the "Agreement") is entered into by and between:

Tarrant County
100 West Weatherford
Fort Worth, TX 76196
Click or tap here to enter text.
("the **Customer**")

and

Siteimprove A/S
Sankt Annæ Plads 28
1250 København K
CVR: 25537017
("the **Supplier**")

have entered into the below Data Processing Agreement ("the **Agreement**") on the Supplier's processing of personal data on the Customer's behalf:

1. General terms

1.1 The Supplier processes personal data for the Customer pursuant to the agreement with the Customer on purchases of the Supplier's online services ("the **Service Agreement**"). The Data Processing Agreement will take precedence over any corresponding or conflicting provisions in the Service Agreement and any other contractual documents.

1.2 The agreement concerns the Supplier's obligation to comply with the requirements for security of processing laid down in 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), which contains specific requirements for the contents of a data processing agreement.

1.3 The Supplier must process personal data in accordance with good data processing practices; see the rules and regulations on processing of personal data in force from time to time, and follow principles and recommendations set forth in ISO 27001.

2. The Customer's rights and obligations

2.1 The Customer must ensure that there is a lawful purpose for the data processing and that the instructions provided by the Customer to the Supplier (see Appendix 3 – Instructions) are in accordance with the General Data Protection Regulation. The Supplier must notify the Customer without undue delay if the Supplier believes that there is no lawful purpose for the data processing.

2.2 The Customer is the Data Controller for the personal data which the Customer instructs the Supplier to process; see clause 4 Instructions of the Agreement.

2.3 The Customer has the rights and obligations vested in a Data Controller pursuant to the legislation; see clause 1.2 of the Agreement.

2.4 The Customer is responsible for ensuring that the personal data that the Customer instructs the Supplier to process may be processed by the Supplier, including that there are no particularly sensitive personal data on the Customer's website.

3. The Supplier's Obligations

3.1 The Supplier is the Data Processor of the personal data processed by the Supplier on the Customer's behalf; see clause 4 Instructions and Appendix 3 – Instructions of the Agreement.

3.2 The Supplier only processes received personal data in accordance with documented instructions from the Customer (see clause 4 Instructions and Appendix 3 – Instructions of the Agreement) and solely for the performance of the Service Agreement.

3.3 The Supplier must continuously keep a record of the processing of personal data as well as a record of all personal data breaches.

3.4 The Supplier must secure the personal data via technical and organizational security measures and in accordance with the General Data Protection Regulation; see Appendix 1 - Security measures in general.

3.5 The Supplier will, taking into account the nature of the processing, assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Data Controller's obligation to respond to requests for exercising the data subject's rights, including responding to requests from citizens about access to their own data, disclosure of the citizen's data, rectification and erasure of data, restriction of processing of the citizen's data, as well as the Customer's obligations in relation to notification of the data subject in the event of personal data breaches.

3.6 The Supplier must assist the Customer in the compliance with the Customer's obligations under Articles 32-36 of the General Data Protection Regulation.

3.7 The Supplier guarantees to provide sufficient expertise, reliability and resources to implement appropriate technical and organizational measures, so that the Supplier's processing of the

Customer's personal data meets the requirements of the General Data Protection Regulation and ensures protection of the data subject's rights.

4. Instructions

4.1 The Supplier will only process personal data on the Customer's behalf in accordance with documented instructions; see Appendix 3 – Instructions. The Supplier is responsible for ensuring that any sub-processors (see clause 5 Sub-supplier (sub-processor)) receive the Customer's instructions; see Appendix 3 – Instructions.

4.2 The Supplier must notify the Customer immediately if the Supplier finds that an instruction is contrary to the General Data Protection Regulation.

5. Sub-supplier (sub-processor)

5.1 A sub-processor is a sub-supplier to which the Supplier has transferred all or parts of the data processing which the Supplier performs on the Customer's behalf.

5.2 The Supplier must not, without the Customer's express written approval, use sub-processors other than those specified in Appendix 2 – Information about locations for processing and sub-suppliers (sub-processors), including replacement of these sub-processors, for processing of the personal data which the Customer has transferred to the Supplier pursuant to the Service Agreement. The Customer cannot refuse to approve the addition or replacement of a sub-processor unless there are specific reasoned grounds for this.

5.3 If the Supplier leaves the processing of personal data for which the Customer is the Data Controller to sub-processors, the Supplier must enter into a written data (sub-)processing agreement with the sub-processor.

5.4 The data sub-processing agreement (see clause 5.3) must impose on the sub-processor the same data protection obligations imposed on the Supplier under the Agreement, including that the sub-processor guarantees to be able to deliver sufficient expertise, reliability, and resources to be able to implement the appropriate technical and organizational measures to ensure that the sub-processors processing meets the requirements of the General Data Protection Regulation and ensures protection of the data subject's rights.

5.5 If the Supplier leaves the processing of personal data for which the Customer is Data Controller to sub-processors, the Supplier is responsible to the Customer for the sub-processors compliance with their obligations; see clause 5.4 of the Agreement.

5.6 The Customer may, at any given time, demand documentation from the Supplier for the existence and contents of data sub-processing agreements for the sub-processors used by the Supplier in connection with the performance of the Supplier's obligations to the Customer.

5.7 All communication between the Customer and the sub-processor will take place via the Supplier.

6. Technical and organizational security measures

6.1 The Supplier must implement all security measures required pursuant to Article 32 of the General Data Protection Regulation, including implementing appropriate technical and organizational security measures to protect personal data from:

6.1.1 destruction, loss, alteration or impairment,

6.1.2 disclosure to unauthorized parties or unauthorized use or from other processing in contravention of the legislation; see clause 1.2 of the Agreement.

6.2 At least once a year, the Supplier must review its internal security regulations and guidelines for processing of personal data to ensure that the necessary security measures are constantly observed; see clause 6.1 and Appendix 1 - Security measures in general of the Agreement.

6.3 The Supplier and its employees are prohibited from obtaining information of any kind which is not relevant to the performance of their tasks.

6.4 The Supplier is obliged to instruct its employees who have access to or otherwise handle the processing of the Customer's personal data, about the Supplier's obligations, including the provisions on a duty of confidentiality; see clause 8 of the Agreement.

6.5 The Supplier is obliged to notify the Customer of any personal data breach immediately after the occurrence thereof.

6.6 The Supplier must not communicate a personal data breach (see clause 6.5 of the Agreement) publicly or to third parties without a prior written agreement with the Customer about the contents of such communication unless the Supplier has a legal obligation to provide such communication.

7. Transfers to other countries

7.1 The Supplier will only transfer personal data to third countries if so instructed by the Customer; see Appendix 3 – Instructions.

7.2 In connection with transfers to third countries, the Supplier and the Customer are jointly responsible for ensuring that there is a valid transfer basis.

7.3 If the Customer's personal data are transferred to an EU Member State, the Supplier is responsible for ensuring that the General Data Protection Regulation's provisions on security measures in force from time to time are complied with.

8. Duty of confidentiality

8.1 During the term of the Service Agreement and after its termination, the Supplier has a duty of complete confidentiality about all information of which the Supplier becomes aware during the cooperation.

8.2 The Supplier must ensure that anyone who is authorized to process personal data covered by the Agreement, including employees, third parties (e.g. a technician), and sub-processors, undertake a duty of confidentiality or are subject to an appropriate statutory duty of confidentiality.

9. Checks and declarations

9.1 The Supplier is obliged to provide the Customer, without undue delay, with the necessary information enabling the Customer to verify at any given time that the Supplier complies with the requirements of this Agreement and Article 28 of the General Data Protection Regulation.

9.2 Once a year, the Supplier must send the Customer a declaration on compliance with this Agreement free of charge. The declaration must be prepared in accordance with ISAE 3000 or an equivalent standard in the area and must include both the Supplier's and any sub-processors data processing. The first declaration must be provided twelve (12) months after the conclusion of the Service Agreement.

9.3 Once a year, the Customer may conduct a physical inspection at the Supplier's premises to verify compliance with this Agreement. The scope and process for the inspection, including the Supplier's price for this, are agreed in the Service Agreement, secondarily in a separate agreement between the parties if the scope and process are not covered by the Service Agreement. The Customer's costs for the inspection are payable by the Customer.

9.4 The Supplier is obliged to grant relevant public authorities which, in accordance with the legislation in force from time to time, have access to the Customer's and Supplier's facilities, or representatives acting on the public authority's behalf, access to the Supplier's physical facilities against presentation of proper identification.

10. Amendments to the Agreement

10.1 The Customer may, at any given time and at minimum thirty (30) days' prior notice, make amendments to the Agreement and the instructions; see Appendix 3 – Instructions. Unless the costs for such amendments are specified in the Service Agreement, and pricing must be agreed before the amendments take effect.

10.2 The Customer is entitled to make amendments to the Agreement at thirty (30) days' notice and without this triggering a claim for payment from the Supplier to the extent to which amendments to legislation (see clause 1.2 of the Agreement) or changes to the established practice give rise to this.

11. Erasure of data

11.1 The Customer decides whether personal data are to be erased or returned after the processing of the personal data has ceased pursuant to the Service Agreement.

11.2 Unless otherwise agreed between the Supplier and the Customer, personal data processed by the Supplier will be erased on termination of this Agreement. If the personal data are instead returned to the Customer, the Supplier must likewise erase any copies. The Supplier must ensure that any sub-processors also comply with the Customer's instructions.

11.3 On the Customer's demand, the Supplier must provide documentation that the demanded data erasure (see clause 11.1 of the Agreement) has been done.

12. Governing law

12.1 This Agreement will be governed by and construed in accordance with the laws of Denmark. In the event of any suit or proceeding arising out of or related to this Agreement, the courts of Denmark, will have exclusive jurisdiction and the parties will submit to the jurisdiction of those courts.

13. Commencement and term

13.1 The Agreement is entered into when signed by both parties and will run until the termination of the Service Agreement or until it is replaced by another valid data processing agreement.

Signatures

By signing this agreement, both parties agree to have read and understood this Agreement in its entirety. The person signing this Agreement represents and warrants that he or she is duly authorized and has the legal capacity to execute this Agreement.

On behalf of Siteimprove A/S:	On behalf of Customer:
Date:2/3/2022	Date:
Jose López Arredondo	
Name: Jose López Arredondo Position: Information Security Manager	Name: Position:

Appendices:

Appendix 1 – Description of the technical and organizational security measures implemented

Appendix 2 – Information about locations for processing and sub-suppliers (sub-processors)

Appendix 3 – Instructions

Appendix 1 Description of the technical and organizational security measures implemented

1. Security measures in general

1.1 Siteimprove will implement and maintain technical and organizational measures to protect the personal data provided by Customers using our product and services against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access as described in this Appendix.

1.2 Siteimprove will continuously improve and develop its security and privacy measures in order to provide appropriate safeguards for protection of personal data. Information Security is organized within its own departmental unit, headed by the Information Security Manager, who is reporting to the Director of Operations and Cloud, striving to improve the quality, reliability, and security of its work and services. Siteimprove may as a result of this ongoing work modify or update practices at its discretion, provided that such modifications and updates do not result in the protection being material degraded. Specific details about the points in this Appendix can be found under References in section 22.

2. Security organization and approach

2.1 Siteimprove has developed a risk-based, holistic and decentralized approach to Information Security and Privacy. Siteimprove acknowledges that risk management is the core of Information Security and that risks must be identified, addressed. and reduced to an acceptable level when discovered.

2.2 By this continuous approach, Siteimprove strives to improve the quality, reliability, and security of its work and services. Information Security is organized within its own departmental unit, headed by the Information Security Manager, who is reporting to the Director of Operations and Cloud.

2.3 Information Security and Privacy responsibilities are delegated throughout the organization to relevant staff such as line managers, process owners, and application owners.

2.4 Siteimprove will take appropriate steps to ensure that employees, contractors, and subprocessors comply with Siteimprove's security policy to the extent applicable taken their scope of performance into account. This includes ensuring that all persons authorized to process personal data provided by the Customer have committed themselves to confidentiality or are under appropriate statutory obligations of confidentiality.

3. Security contact

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

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

4. Vendor Management

4.1 In order to conduct business effectively, Siteimprove collaborates with various vendors. When choosing to collaborate with a vendor or to use new hardware and software, Siteimprove assesses the criticality and risks to the products and services provided by the vendor. **This process is known as the "Vendor Management Process" within Siteimprove and it is a joint initiative between the Legal, Information Security, IT, and Finance departments.**

4.2 Siteimprove makes sure to commit any vendor to confidentiality and confidentiality clauses are a standard requirement in our supplier contracts. Data Processing Agreements and contractual model clauses are used to further ensure a secure collaboration.

4.3 **The relationship with the vendor and associated documentation is inspected every year as part of an internal security audit.**

5. Security incidents

5.1 As part of the Information Security policy, Siteimprove holds and maintains a Security Incident Response Plan based on guidelines from NIST (800-61). A security incident is an event for which there is a greater likelihood that data has left, or will leave, Siteimprove, but uncertainty remains about whether unauthorized acquisition or access has occurred. A security incident either has had, can have, or will have a negative impact on the confidentiality, integrity, and availability of Siteimprove informational and technological assets.

5.2 Examples of security incidents include:

5.2.1 Virus/ransomware infection

5.2.2 Suspicious activity on company devices or accounts

5.2.3 Former employee suspected of accessing Siteimprove network or tools after contract termination.

5.3 Security incidents generally require further investigation to determine whether data or assets were improperly accessed or acquired (i.e. whether the incident could be classified as a breach). To aid in the investigation, security incidents are classified and handled with a priority based on the impact to the business and associated assets:

5.3.1 Critical - related to critical assets or situations that can lead to a disaster.

5.3.1.1 Handling: As soon as possible following notification/identification and solved as soon as possible

5.3.1.2 Example: Ransomware infection on multiple subnets with a big probability to infect development or production servers

5.3.2 High - related to important assets or situations that can lead to a disaster.

5.3.2.1 Handling: Within two (2) hours of notification/identification and solved as soon as possible

5.3.2.2 Example: Ransomware infection on an isolated network segment

5.3.3 Medium - related to generic assets and situations affecting multiple users.

5.3.3.1 Handling: Within one (1) business day and solved within seven (7) business days

5.3.3.2 Example: Multiple user endpoints infected with adware

5.3.4 Low - related to generic assets and situation affecting one user.

5.3.4.1 Handling: Within three (3) business days and solved within ten (10) business days

5.3.4.2 Example: User endpoint infection with adware

5.4 The Security Incident Response Plan serves not only to address a specific security incident but also to provide critical input in the preparation against subsequent incidents. The main phases of the Security Incident Response plan are listed below:

5.4.1 Preparation

5.4.2 Identification

5.4.3 Containment

5.4.4 Investigation

5.4.5 Eradication

5.4.6 Recovery

5.4.7 Reporting

5.4.8 Lessons learned

5.5 Siteimprove commits to a notification via email to affected data controllers -customers/partners-, specifically to the primary business contact registered upon contract signing, as soon as possible but no later than 48 hours of reasonable suspicion of a Data Breach. If there is an operational impact, updates will appear on status.siteimprove.com as well.

6. Pseudonymization and encryption

6.1 Siteimprove assures the confidentiality and integrity of personal data by using and supporting the latest recommended secure cipher suites and protocols for encryption.

6.2 Concerning Data in transit - The Siteimprove Intelligence Platform is only accessible using HTTPS on TLS 1.2.

6.3 Concerning Data at rest - User passwords are salted and hashed using SHA512. Confidential Customer data is encrypted using Transparent Data Encryption (TDE).

6.4 Pseudonymization is applied wherever feasible, by separating direct and indirect identifiers, in order to facilitate secure and private processing. Likewise, data is logically segregated in order to ensure confidentiality of the information.

7. Data retention and backup

7.1 Siteimprove will store personal data provided by the Customer:

7.1.1 As long as the Agreement between Siteimprove and Customer stands, we process and retain the personal data provided by the Customer.

7.1.2 As soon as the Agreement between Siteimprove and Customer is terminated, we initiate the deletion of the specific personal data provided by the Customer, thus the retention period for the Customer ends.

7.2 However, Siteimprove will retain some information about the Customer after the contract termination, due to legal and financial requirements.

7.3 When the Agreement between Siteimprove and Customer is terminated, the following will happen:

7.3.1 The tables in the database, containing the customer results, history, and specific customizations to the Siteimprove Suite will be dropped.

7.3.2 Crawled website data (HTML) and/or any linked documents (such as PDF files) will be deleted.

7.3.3 Elimination from the backup scheme is initiated; due to the backup frequency and the technical setup, personal data will be fully rolled out of the backup scheme thirty (90) days after initiation.

7.4 Backup of personal data is completed on a regular and frequent basis, depending on the data in scope. Backup material is encrypted and transferred to an offsite location, which is part of Siteimprove's infrastructure.

7.5 Personal data belonging to Customers within the EU will be stored, processed, and backed up in the EU components of the Siteimprove infrastructure.

8. Physical security

8.1 Siteimprove maintains geographically distributed data centers. Siteimprove stores all production data in physically secure data centers.

9. Interxion

9.1 Interxion is a ISO 27001:2013 (Information Security) and ISO 22301:2012 (Business continuity) certified data center provider. Interxion also undergoes a yearly SOC2 audit. Both the certificates and the audit report can be provided to customers, upon request.

9.2 Further information about Interxion can be found on their official website.

9.3 Only a limited number of named Siteimprove employees have physical access to the data center.

10. Amazon Web Services

10.1 AWS is a multi-certified data center provider, including certifications ISO 27001:2013(Information Security) and SOC 1, 2, and 3.

10.2 Further information about AWS security posture can be found on their official website.

10.3 AWS in Frankfurt, Germany is used by Siteimprove for storage of PDF and HTML files collected by the Quality Assurance service. It is also used for storage of Response website snapshots.

10.4 AWS is used for off-loading application servers located in Interxion.

11. Siteimprove's access to personal data provided by the Customer

11.1 The operation of Siteimprove services requires that some employees have access to the systems that store and process personal data provided by the Customer. These employees are prohibited from using these permissions to view the data unless it is a necessity. Technical controls and audit policies are in place and reviewed on a yearly basis to ensure that any access to personal data provided by the Customer is controlled and logged.

11.2 Employee access to sensitive or critical information processing facilities is managed in accordance with the "need to know and least privilege" principles, ensuring that access is granted only to resources that require it to perform their tasks. The assessment of granting access privileges must be based upon current job function responsibilities.

11.3 Employees' passwords are protected according to current industry best practices (NIST 800-63), including an annual review of users in order to check correct operations. 2FA authentication using TOTP is implemented wherever technically feasible and Siteimprove currently uses it for all users accessing the email system used to communicate with customers and for all users using the Siteimprove Customer Relationship Management software.

11.4 User 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.

11.5 Logs are inspected as part of the internal security audit as well as external audits relevant to the specific area of logging (infrastructure supporting financial activities or infrastructure supporting product development).

12. User management within the Siteimprove suite

12.1 The customer is responsible for user management within the Siteimprove services. Access roles and rights within the application are predefined and detailed in the User Roles Right 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.

12.2 Regarding authentication, the platform uses its own repository of users with local authentication. It is possible to configure Single Sign On (SSO) depending on the selection of Siteimprove's Technical Support Schemes available. Session hijacking is prevented by encryption in transit of the session, applying the "secure" flag to the session cookie.

13. Personnel practices and Security Awareness

13.1 Prior to employment with Siteimprove, candidates will be assessed and checked on their background, considering the position they will hold and the applicable law and regulations. Siteimprove has offices in many locations around the world and has HR resources who are familiar with local requirements. Criminal checks of employees prior to starting are normally only done for US employees.

13.2 Employees will be made aware of Security threats and practices during onboarding as well as on an ongoing basis, including the completion of the mandatory data protection training which includes data privacy contents. Upon employment, the employee signs the IT policy and Code of Conduct acknowledging that they have read and understood the document which is the basic set of rules which all employees must comply with, including the acceptable use of devices and networks.

13.3 All personnel is required to sign a Confidentiality Agreement as a condition of employment.

13.4 Any violation to Siteimprove policies, procedures, or code of conduct may result in disciplinary actions.

14. Network and host protection

14.1 To ensure the protection of information in networks, 2nd generation firewall is installed with Deep packet inspection (DPI) and Intrusion Prevention System (IPS).

14.2 Siteimprove uses industry-standard endpoint protection which relies on signature and heuristic-based detection. Servers are restricted to run only the services they are intended to.

15. Patch management

15.1 For user endpoints, Siteimprove has 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 our computing devices, applications, and systems. Patches are assessed before applied to production infrastructure equipment to minimize the risk of service disruption.

16. Service and data availability

16.1 The continuous operation of the services delivered by Siteimprove is reliant on the systems and infrastructure owned by Siteimprove as well as third parties who provide hosting or supporting services. IT infrastructure, Operations, and Development staff are monitoring the Siteimprove infrastructure for any risks that can affect the availability of the Siteimprove services. Core

business systems run on Virtual Machines on High Availability infrastructure. The hardware used to house core business systems have redundant components.

16.2 Given the nature and implications of data security, data privacy, and information technology, Siteimprove cannot guarantee 100% availability to its services. To cover this gap, Siteimprove has prepared response procedures that can be invoked in case of an event that can affect the availability of the services.

16.3 In case of an availability issue: should any Service or any Service function or component not be available, Siteimprove will: (i) verify the outage; (ii) if the outage is verified, notify Customer as long as Customer has signed up for email alerts at https://status.siteimprove.com; (iii) resolve the outage or, if determined to be a matter that is not directly controllable, such as an internet provider problem, open a ticket with the internet provider; and notify Customer when the outage has been resolved, along with any pertinent findings.

16.4 In case of hardware failure: an agreement is in place with a provider that will replace failing hardware components in a short amount of time. Siteimprove Platform status can be checked on status.siteimprove.com

16.5 For Siteimprove's own systems and infrastructure, a Business Impact Assessment has been completed, defining the business-critical systems. Siteimprove maintains a Master Disaster Recovery Plan that is directly linked with individual Disaster Recovery plans for critical systems place which consist of documented technical procedures that will restore Siteimprove services in case of an outage. The plan is reviewed and tested on an annual basis.

16.6 Siteimprove also has a Business continuity plan in place which consists of documented organizational procedures and processes to be implemented during a Crisis to allow business operations to continue. During a Crisis, the goal of the Plan is to ensure information system uptime; data integrity and availability; and business continuity. The plan is set to be reviewed and tested on an annual basis.

17. Working remotely

17.1 Siteimprove employees are allowed to work remotely only when using a Siteimprove managed device (work laptop) and a Siteimprove approved connection to Siteimprove systems (VPN). Alternatives are not allowed nor technically possible.

18. Logging

18.1 Logging is used to troubleshoot and monitor Siteimprove systems for abnormal functional patterns, suspicious behavior, and other activities incompliant with the existing legislation and Information Security policy. Customer data access logs are reviewed as part of an incident and as part of the annual Internal Security Audit.

18.2 Logs are centralized into separate information systems, which only staff with a relevant business need has access to, and is limited to staff from Information Security, IT support, IT infrastructure, Operations, and Development departments. Logs are kept for as long as needed from a business perspective.

19. Data collection and cookies

19.1 When it comes to Siteimprove Analytics, Siteimprove collects customer website visitor analytics data via the script on your website, which passes information through our endpoints to datacenters. These endpoints are located based on customer location so that collection is done more efficiently.

19.2 To make the website and other communications related to Siteimprove services work properly, we place small text files (cookies) on your device when you visit our website. For more information about the usage of cookies, please visit https://support.siteimprove.com/hc/en-gb/articles/115000070092-Analytics-Technical-Specifications.

20. GDPR compliance

20.1 Siteimprove is committed to GDPR compliance in both its own internal processing of personal data as well as customer-use of the Siteimprove Intelligence Platform. For further information on this matter please visit Siteimprove's GDPR Compliance webpage.

21. Regular testing and evaluation of the effectiveness of the technical and organizational security measures

21.1 Internal security audit. In order to properly implement the Siteimprove Information Security policy, the Internal Security Audit is conducted every year, with the objectives of (i) assuring adherence to the Information Security Policy and other underlying policies, (ii) monitor and follow-up on regulatory information security requirements relevant to Siteimprove (e.g. personal data processing), (iii) Identify new risks and (iv) Indirectly raise employee awareness around Security and Privacy.

21.2 External security audit. Siteimprove undergoes yearly security audits from third parties to obtain an objective view over the effectiveness of the technical and organizational security measures.

21.3 Financial audit. Due to financial regulatory requirements, Siteimprove undergoes a Financial audit on a yearly basis. The IT infrastructure related to the financial data processing is included in the audit and servers as an additional, external, objective method of assessing and evaluating the effectiveness of the technical and organizational security measures.

21.4 Penetration testing and vulnerability management. To continuously assure a reliable and secure product for Customers, Siteimprove has its application suite tested for security vulnerabilities, both internally and externally.

21.4.1 Internally, this is done through quality checks before each release as well as 'bug hunting' sessions, where Siteimprove's developers will try out new features to discover if the application is not responding as it should.

21.4.2 Externally, this is done annually by a third-party party entity that specializes in penetration testing services which performs an annual assessment of OWASP top 25 vulnerabilities.

21.4.3 The process concludes with a vulnerability report which serves as input for the development of the application. Siteimprove, as with any other software developer company or cloud provider, cannot fully guarantee the lack of specific vulnerabilities due to the nature of the field – but Siteimprove does apply a reasonable amount of effort to prevent, identify and remediate vulnerabilities.

21.5 Code development and review. We follow Agile development methodology which help us to provide a quick and proper answer to any feedback given by our customers or internal quality assurance tests, assessing continuously the direction of the project during its development cycle. Our code runs through multiple individual (unit testing), automated (multiple tests in the CI/CD pipeline), and manual tests (through internal peer-review), and transitions through the development and staging environments, before being deployed to production.

21.6 Reviews of Security Documentation. After the parties have entered into a Non-Disclosure Agreement (NDA) Siteimprove will enable the Customer to review the following documents and information to demonstrate compliance with Siteimprove's obligations:

21.6.1 the certificates issued for Siteimprove infrastructure providers in relation to the ISO 27001 Certification, the ISO 22301 Certification

21.6.2 the then-current SOC 2 Report for Siteimprove infrastructure providers

21.6.3 the then-current Penetration testing attestation for the Siteimprove Intelligence Platform

21.6.4 the Siteimprove Business Continuity Plan

21.6.5 the Siteimprove Master Disaster Recovery Plan

22. References

https://siteimprove.com/en/privacy/

https://siteimprove.com/en/privacy/data-breach-policy/

https://siteimprove.com/en/privacy/vulnerability/

https://siteimprove.com/en/privacy/information-security-notice/

https://siteimprove.com/en/privacy/privacy-policy/

https://siteimprove.com/en/privacy/website-privacy-policy/

https://siteimprove.com/en/privacy/gdpr-compliance/

Appendix 2 – Information about locations for processing and sub-suppliers (sub-processors)

This Annex constitutes Siteimprove's disclosure to Customer of sub-processors used to provide the Included Services. It is an integrated part of the Agreement and its inclusion constitutes Customer's agreement to the use of said sub-processors.

1. Interxion

1.1 Siteimprove uses Interxion, located in Industriparken 20A DK, 2750 Ballerup, Denmark, is the primary hosting location for the Siteimprove infrastructure. This location contains the bulk of the Siteimprove application logic and the various database back-ends. Only a limited number of named Siteimprove employees have physical access to the data center.

Interxion is a state-of-the-art data center provider with:

1.1.1 Power delivery with 99.999% SLA
1.1.2 Temperature and humidity is monitored 24x7 and is in line with ASHRAE recommendations
1.1.3 Diverse ISP connectivity
1.1.4 A very early smoke detection system is installed with direct lines to fire stations
1.1.5 Automatic gas-based fire suppression systems
1.1.6 Fire-retardant walls
1.1.7 Trained security staff on site 24x7
1.1.8 Five layers of physical security
1.1.9 Access tokens in combination with biometric data and mantraps are used for data center entry
1.1.10 CCTV video surveillance

1.2 Interxion has access procedures in place for personnel and goods entry and maintains an access log for all entry to the data center.

1.3 Interxion is a ISO 27001:2013 (Information Security) and ISO 22301:2012 (Business continuity) certified data center provider. Interxion does also undergo a yearly SOC2 audit. Both the certificates and the audit report can be provided to customers, upon request.

1.4 Further information about Interxion can be found on their website at www.interxion.com/locations/denmark/copenhagen/

2. Amazon Web Services (AWS)

2.1 Siteimprove also uses AWS Frankfurt, Germany to host some of our service components, which mainly relates to the storage of crawled content and PDF files collected from Customers' websites by the Quality Assurance service and storage of Response website snapshots. AWS is also the main locating for processing of Analytics data.

2.2 AWS is also used for off-loading application servers located in Interxion. When certain thresholds are met, workloads are moved to AWS for processing, after which, the processed data is returned to Interxion.

2.3 AWS is considered one of the top providers of cloud services and hold a number of certifications and are on a yearly basis subjected to several independent audits in order to maintain the certifications. AWS website: https://aws.amazon.com/compliance/.

Appendix 3 – Instructions

1. Instructions

1.1 The Customer hereby instructs the Supplier to process the Customer's data for use for operation and maintenance of the Customer's website and to form an overview of the website traffic; see the Service Agreement.

1.2 If the Supplier leaves the processing of the Customer's data to sub-processors, the Supplier is responsible for entering into written data (sub-)processing agreements with these; see clause 5.4. The Supplier is responsible for ensuring that the Customer's instructions are sent to any sub-processors.

2. Purpose of the processing

2.1 The Supplier is a multinational software-as-a-service provider which gives customers access to cloud-based tools and services that automate the process of identifying errors, faults and deficiencies on websites. The Supplier's Intelligence Platform constitutes a collection of integrated tools for management and optimization of website content, improvement of search engine optimization (SEO), monitoring of website performance and/or use of website analysis data. The Customer has purchased access to such services.

3. General description of data processing

3.1 The Supplier'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, the Supplier collects and processes both personally attributable and not personally attributable data on the Customer's website in connection with the provision of the services. If using Siteimprove Analytics, IP addresses of visitors to the Customer's website will also be processed. Customer has the opportunity to use IP anonymization which means IP addresses will only be processed to the extent necessary to deliver essential parts of the Analytics services and to the extent technical necessary. After collection of IP addresses, they will be anonymized and thereby not traceable in the Platform.The Supplier does not sell the processed data to a third party.

4. Type of Personal data

4.1 The data processing comprises personal data in the categories ticked below. The Supplier's and any sub-processors' level for security of processing should reflect the data sensitivity.

Ordinary personal data (see Article 6 of the General Data Protection Regulation)

☒ Ordinary personal data

Sensitive personal data (see Article 9 of the General Data Protection Regulation)

☐ 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 General Data Protection Regulation):

☐ Criminal convictions and offences
☐ Serious social problems
☐ Other purely private matters which are not mentioned above:

_____

_____

Data about civil registration number (see Article 87 of the General Data Protection Regulation)

☐ Civil registration numbers

5. Categories of data subjects

5.1 Data are processed about the following categories of data subjects (e.g. citizens, students, welfare benefit recipients, et al.):

5.1.1 Any person who may be stated or identifiable on the Customer's website.

6. Third countries (non-EU member states)

6.1 The Supplier does not transfer to third countries personal data which the Supplier processes as part of the provision of the Supplier's services.

Siteimprove

CCPA DATA PROCESSING AGREEMENT

Between

Tarrant County
100 West Weatherford
Fort Worth, TX 76196

('the Customer')

and

Siteimprove, Inc.
7807 Creekridge Circle
Minneapolis, MN 55439
('the Supplier')

have entered into the below CCPA Data Processing Agreement ('the CCPA DPA') on the Supplier's processing of Personal Information on the Customer's behalf:

1. General terms

1.1 The Supplier processes Personal Information for the Customer pursuant to the agreement with the Customer on purchases of the Supplier's online services ('the Service Agreement'). The CCPA DPA will take precedence over any corresponding or conflicting provisions in the Service Agreement.

1.2 The CCPA DPA concerns the Supplier's obligation to comply with the requirements for processing Personal Information set forth in the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq., ("CCPA").

1.3 Capitalized terms identified in this CCPA DPA shall have the same meaning as defined in the CCPA, unless otherwise noted.

2. The Customer's rights and obligations

2.1 The Customer is the Business for the Personal Information which the Customer instructs the Supplier to process; see Clause 4 of the CCPA DPA.

2.2 The Customer has the rights and obligations vested in a Business pursuant to the CCPA; see Clause 1.2 of the CCPA DPA.

2.3 The Customer is responsible for ensuring that the Personal Information that the Customer instructs the Supplier to process may be processed by the Supplier, including that there are no particularly sensitive Personal Information on the Customer's website.

3. The Supplier's obligations

3.1 The Supplier is the Service Provider of the Personal Information processed by the Supplier on the Customer's behalf; see Clause 4 and Appendix 3 of the CCPA DPA.

3.2 The Supplier only processes received Personal Information in accordance with documented instructions from the Customer (see Clause 4 and Appendix 3 of the CCPA DPA) and solely for the performance of the Service Agreement.

3.3 The Supplier must continuously keep a record of the processing of Personal Information.

3.4 The Supplier must secure the Personal Information via technical and organizational security measures; see Appendix 1 – Security.

3.5 The Supplier will, taking into account the nature of the processing, assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation as a Business to respond to requests for exercising the Consumer's rights.

3.6 The Supplier shall not Sell Personal Information.

4. Instructions and Assisting with Customer's CCPA Obligations

4.1 The Supplier will only process Personal Information on the Customer's behalf in accordance with documented instructions; see Appendix 3. The Supplier is responsible for ensuring that any sub-processors (see Clause 5 of the CCPA DPA) receive the Customer's instructions; see Appendix 3.

4.2 The Supplier shall cooperate with Customer if a Consumer requests (i) access to his or her Personal Information, (ii) information about the categories of sources from which the Personal Information is collected, or (iii) information about the categories or specific pieces of the individual's Personal Information, including by providing the requested information in a portable and, to the extent technically feasible, readily useable format that allows the Consumer to transmit the information to another entity without hindrance.

4.3 The Supplier shall inform Customer in writing within three (3) business days of any requests it receives from individuals with respect to their Personal Information. The Supplier also shall direct the requesting individual to submit the request directly to Customer by contacting Customer as described in Customer's then-current privacy policy.

4.4 Upon Customer's request, the Supplier shall promptly delete a particular individual's Personal Information from Supplier's records. In the event Supplier is unable to delete the Personal Information for reasons permitted under the CCPA, Supplier shall (i) promptly inform Customer of the reason(s) for its refusal of the deletion request, (ii) ensure the privacy, confidentiality and security of such Personal Information, and (iii) delete the Personal Information promptly after the reason(s) for Supplier's refusal has expired.

5. Sub-supplier (sub-processor)

5.1 A sub-processor is a sub-supplier to which the Supplier has transferred all or parts of the processing of Personal Information which the Supplier performs on the Customer's behalf.

5.2 The Supplier must not, without the Customer's express written approval, use sub-processors other than those specified in Appendix 2, including replacement of these sub-processors, for processing of the Personal Information which the Customer has transferred to the Supplier pursuant to the Service Agreement. The Customer cannot refuse to approve addition or replacement of a sub-processor unless there are specific reasoned grounds for this.

5.3 If the Supplier leaves the processing of Personal Information for which the Customer is the Business to sub-processors, the Supplier must enter into a written data (sub-)processing agreement with the sub-processor.

5.4 The data sub-processing agreement (see Clause 5.3 of the CCPA DPA) must impose on the sub-processor the same data protection obligations imposed on the Supplier under this CCPA DPA, including that the sub-processor guarantees to be able to deliver sufficient expertise, reliability and resources to be able to implement the appropriate technical and organizational measures.

5.5 If the Supplier leaves the processing of Personal Information for which the Customer is the Business to sub-processors, the Supplier is responsible to the Customer for the sub-processors' compliance with their obligations; see Clause 5.4 of the CCPA DPA.

5.6 All communication between the Customer and the sub-processor will take place via the Supplier.

6. Technical and organizational security measures

6.1 The Supplier shall comply with all applicable provisions of the CCPA, including implementing and maintaining reasonable security measures to safeguard any Personal Information that the Customer discloses to Supplier under the Service Agreement.

6.2 The Supplier is obliged to instruct its employees who have access to or otherwise handle the processing of the Customer's Personal Information, about the Supplier's obligations, including the provisions on a duty of confidentiality; see Clause 8 of the CCPA DPA.

7. Duty of confidentiality

7.1 During the term of the Service Agreement and after its termination, the Supplier has a duty of complete confidentiality about all Personal Information of which the Supplier becomes aware during the cooperation.

7.2 The Supplier must ensure that anyone who is authorized to process Personal Information covered by the CCPA DPA, including employees, third parties (e.g. a technician) and sub-processors, undertake a duty of confidentiality or are subject to an appropriate statutory duty of confidentiality.

8. Amendments to the CCPA DPA

8.1 The Customer may, at any given time and at minimum 30 days' prior notice, make amendments to the CCPA DPA and the instructions; see Appendix 3. Unless the costs for such amendments are specified in the Service Agreement, any pricing must be agreed before the amendments take effect.

9. Governing law

9.1 This CCPA DPA will be governed by and construed in accordance with the laws of California. In the event of any suit or proceeding arising out of or related to this CCPA DPA, the courts of California will have exclusive jurisdiction and the parties will submit to the jurisdiction of those courts.

10. Commencement and term

10.1 The CCPA DPA is entered into when signed by both parties and will run until the termination of the Service Agreement or until it is replaced by another valid CCPA data processing agreement.

Siteimprove

SIGNATURES

By signing below, each party acknowledges that it has carefully read and agrees to be bound by the terms of this CCPA DPA. This CCPA DPA will become effective on the last date signed.

CUSTOMER

Signature

_____

Tarrant County

Date

03/02 2022

SITEIMPROVE INC.

Signature

Jose López Arredondo

Information Security Manager

Date

03/02 2022

Appendices:

Appendix 1 – Description of the technical and organizational security measures implemented

Appendix 2 – Information about locations for processing and sub-suppliers (sub-processors)

Appendix 3 – Instructions

Siteimprove

Appendix 1 Description of the technical and organizational security measures implemented

1.1. Security measures in general

Siteimprove will implement and maintain technical and organizational measures to protect the Personal Information provided by Customers using our product and services against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in this Appendix.

Siteimprove will continuously improve and develop its security and privacy measures in order to provide appropriate safeguards for protection of Personal Information. Information Security is organized within its own departmental unit, headed by the Information Security Manager, who is reporting to the Director of Operations and Cloud, striving to improve the quality, reliability and security of its work and services. Siteimprove may as a result of this ongoing work modify or update practices at its discretion, provided that such modifications and updates do not result in the protection being material degraded. Specific details about the points in this Appendix can be found Under References in section 20.

1.2. Security organization and approach

Siteimprove has developed a risk-based, holistic and decentralized approach to Information Security and Privacy. Siteimprove acknowledges that risk management is the core of Information Security and that risks must be identified, addressed and reduced to an acceptable level when discovered.

By this continuous approach, Siteimprove strives to improve the quality, reliability and security of its work and services. Information Security is organized within its own departmental unit, headed by the Information Security Manager, who is reporting to the Director of Operations and Cloud.

Information Security and Privacy responsibilities are delegated throughout the organization to relevant staff such as line managers, process owners and application owners.

Siteimprove will take appropriate steps to ensure that employees, contractors and subprocessors comply with Siteimprove's security policy to the extent applicable taken their scope of performance into account. This includes ensuring that all persons authorized to process Personal Information provided by the Customer have committed themselves to confidentiality or are under appropriate statutory obligations of confidentiality.

1.3. Security contact

The single point of contact for Siteimprove security matters is the Siteimprove Information Security Manager:

Victor Alexandru Truica - vat@siteimprove.com

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

1.4. Vendor management

In order to conduct business effectively, Siteimprove collaborates with various vendors. When choosing to collaborate with a vendor or to use new hardware and software, Siteimprove assesses the criticality and risks to the products and services provided by the vendor. **This process is known as the "vendor management process" within Siteimprove and it is a joint initiative between the Legal, Information Security, IT and Finance departments.**

Siteimprove makes sure to commit any vendor to confidentiality and confidentiality clauses is a standard requirement in our supplier contracts. Data Processing Agreements and contractual model clauses are used to further ensure a secure collaboration.

The relationship with the vendor and associated documentation is inspected every year as part of internal security audit.

1.5. Security incidents

As part of the Information Security policy, Siteimprove holds and maintains a Security Incident Response Plan based on guidelines from NIST (800-61).A security incident is an event for which there is a greater likelihood that data has left, or will leave, Siteimprove, but uncertainty remains about whether unauthorized acquisition or access has occurred.

A security incident either has had, can have, or will have a negative impact on the confidentiality, integrity and availability of Siteimprove informational and technological assets.

Examples of security incidents include:

- Virus/ransomware infection
- Suspicious activity on company devices or accounts
- Former employee suspected of accessing Siteimprove network or tools after contract termination

Security incidents generally require further investigation to determine whether data or assets were improperly accessed or acquired (i.e. whether the incident could be classified as a breach). To aid in the investigation, security incidents are classified and handled with a priority based on the impact to the business and associated assets:

- Critical - related to critical assets or situations that can lead to a disaster
    - Handling: As soon as possible following notification/identification and solved as soon as possible
    - Example: Ransomware infection on multiple subnets with a big probability to infect development or production servers
- High - related to important assets or situations that can lead into a disaster
    - Handling: Within 2 hours of notification/identification and solved as soon as possible
    - Example: Ransomware infection on an isolated network segment
- Medium - related to generic assets and situation affecting multiple users
    - Handling: Within 1 business day and solved within 7 business days
    - Example: Multiple user endpoints infected with adware
- Low - related to generic assets and situation affecting one user
    - Handling: Within 3 business days and solved within 10 business days
    - Example: User endpoint infection with adware

The Security Incident Response Plan serves not only to address a specific security incident, but also to provide critical input in the preparation against subsequent incidents. The main phases of the Security Incident Response plan are listed below:

- Preparation
- Identification
- Containment
- Investigation
- Eradication
- Recovery
- Reporting
- Lessons learned

Siteimprove commits to a notification via email to affected data controllers -customers/partners-, specifically to the primary business contact registered upon contract signing, as soon as possible but no later than 48 hours of reasonable suspicion of a Data Breach. If there is an operational impact, updates will appear on status.siteimprove.com as well.

1.6. Pseudononymization and encryption

Siteimprove assures the confidentiality and integrity of Personal Information by using and supporting the latest recommended secure cipher suites and protocols for encryption.

Concerning Data in transit - The Siteimprove Intelligence Platform is only accessible using HTTPS on TLS 1.2.

Concerning Data at rest - User passwords are salted and hashed using SHA512. Confidential Customer data is encrypted using Transparent Data Encryption (TDE).

Pseudononymization is applied wherever feasible, by separating direct and indirect identifiers, in order to facilitate secure and private processing. Likewise, data is logically segregated in order to ensure confidentiality of the information.

1.7. Data retention and backup

Siteimprove will store Personal Information provided by the Customer:

- As long as the Agreement between Siteimprove and Customer stands, we process and retain the Personal Information provided by the Customer.
- As soon as the Agreement between Siteimprove and Customer is terminated, we initiate deletion of the specific Personal Information provided by the Customer, thus the retention period for the Customer ends.

However, Siteimprove will retain some information about the Customer after contract termination, due to legal and financial requirements.

When the Agreement between Siteimprove and Customer is terminated, the following will happen:

- The tables in the database, containing the customer results, history and specific customizations to the Siteimprove Suite will be dropped
- Crawled website data (HTML) and/or any linked documents (such as PDF files) will be deleted

- Elimination from backup scheme is initiated; due to the backup frequency and the technical setup, Personal Information will be fully rolled out of the backup scheme 30 days after initiation

Backup of Personal Information is completed on a regular and frequent basis. Critical customer information is backed up 3 times per day and backup of crawl contents and application settings is done on a weekly basis. Backup material is encrypted and transferred to an offsite location, which is part of Siteimprove's infrastructure.

Personal Information belonging to Customers will be stored, processed and backed up in the EU components of the Siteimprove infrastructure.

1.8. Physical security

Siteimprove maintains geographically distributed data centers. Siteimprove stores all production data in physically secure data centers.

Interxion

Interxion is a ISO 27001:2013(Information Security) and ISO 22301:2012(business continuity) certified data center provider. Interxion does also undergo a yearly SOC2 audit. Both the certificates and the audit report can be provided to customers, upon request.

Further information about Interxion can be found on their official website.

Only a limited number of named Siteimprove employees have physical access to the data center.

Amazon Web Services

AWS is a multi-certified data center provider, including certifications ISO 27001:2013(Information Security) and SOC 1, 2 and 3.

Further information about AWS security posture can be found on their official website.

AWS in Frankfurt, Germany is used by Siteimprove for storage of PDF and HTML files collected by the Quality Assurance service. It is also used for storage of Response website snapshots.

AWS is used for off-loading application servers located in Interxion.

1.9. Siteimprove's access to Personal Information provided by the Customer

The operation of Siteimprove services requires that some employees have access to the systems that store and process Personal Information provided by the Customer. These employees are prohibited from using these permissions to view the data unless it is a necessity. Technical controls and audit policies are in place and reviewed on a yearly basis to ensure that any access to Personal Information provided by the Customer is controlled and logged.

Employee access to sensitive or critical information processing facilities is managed in accordance with the "need to know and least privilege" principles, ensuring that access is granted only to resources that require it to perform their tasks. The assessment of granting access privileges must be based upon current job function responsibilities.

Employees' passwords are protected according to current industry best practices (NIST 800-63), including an annual review of users in order to check correct operation. 2FA authentication using TOTP is implemented wherever technically feasible and Siteimprove currently uses it for all users accessing the email system used to communicate with customers and for all users using the Siteimprove Customer Relationship Management software.

User activities related to Personal Information 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 technical feasible.

Logs are inspected as part of the internal security audit as well as external audits relevant to the specific area of logging (infrastructure supporting financial activities or infrastructure supporting product development).

1.10. User management within the Siteimprove suite

The customer is responsible for user management within the Siteimprove services. Access roles and rights within the application are predefined and detailed in the User Roles Right 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 to configure Single Sign On (SSO) depending on the selection of Siteimprove's Technical Support Schemes available. Session hijacking is prevented by encryption in transit of the session, applying the "secure" flag to the session cookie.

1.11. Personnel practices and Security Awareness

Prior to employment with Siteimprove, candidates will be assessed and checked on their background, considering the position they will hold and the applicable law and regulations. Siteimprove has offices in many locations around the world and has HR resources who are familiar with local requirements. Criminal checks of employees prior to starting are normally only done for US employees.

Employees will be made aware of Security threats and practices during onboarding as well as on an ongoing basis, including the completion of the mandatory data protection training which includes data privacy contents. Upon employment, the employee signs the IT policy and Code of Conduct acknowledging that they have read and understood the document which is the basic set of rules which all employees must comply with, including the acceptable use of devices and networks.

All personnel are required to sign a Confidentiality Agreement as a condition of employment.

Any violation to Siteimprove policies, procedures or code of conduct may result in disciplinary actions.

1.12. Network and host protection

To ensure protection of information in networks, 2nd generation firewall is installed with Deep packet inspection (DPI) and Intrusion Prevention System (IPS).

Siteimprove uses industry standard endpoint protection which relies on signature and heuristic based detection. Servers are restricted to run only the services they are intended to.

1.13. Patch management

For user endpoints, Siteimprove has 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 our computing devices,

applications and systems. Patches are assessed before applied to production infrastructure equipment to minimize the risk of service disruption.

1.14. Service and data availability

The continuous operation of the services delivered by Siteimprove is reliant on the systems and infrastructure owned by Siteimprove as well as third parties who provide hosting or supporting services. IT infrastructure, Operations and Development staff are monitoring the Siteimprove infrastructure for any risks that can affect the availability of the Siteimprove services. Core business systems run on Virtual Machines on High Availability infrastructure. The hardware used to house core business systems have redundant components.

Given the nature and implications of data security, data privacy and information technology, Siteimprove cannot guarantee 100% availability to its services. To cover this gap, Siteimprove has prepared response procedures that can be invoked in case of an event that can affect the availability of the services.

In case of an availability issue: should any Service or any Service function or component not be available, Siteimprove will: (a) verify the outage; (b) if the outage is verified, notify Customer as long as Customer has signed up for email alerts at https://status.siteimprove.com; (c) resolve the outage or, if determined to be a matter that is not directly controllable, such as an internet provider problem, open a ticket with the internet provider; and notify Customer when the outage has been resolved, along with any pertinent findings.

In case of hardware failure: an agreement is in place with a provider that will replace failing hardware components in a short amount of time. Siteimprove Platform status can be checked on status.siteimprove.com

For Siteimprove's own systems and infrastructure, a Business Impact Assessment has been completed, defining the business-critical systems. Siteimprove maintains a Master Disaster Recovery Plan that is directly linked with individual Disaster Recovery plans for critical systems place which consist of documented technical procedures that will restore Siteimprove services in case of an outage. The plan is reviewed and tested on an annual basis.

Siteimprove also has a Business continuity plan in place which consists of documented organizational procedures and processes to be implemented during a Crisis to allow business operations to continue. During a Crisis, the goal of the Plan is to ensure information system uptime; data integrity and availability; and business continuity. The plan is set to be reviewed and tested on an annual basis.

1.15. Working remotely

Siteimprove employees are allowed to work remotely only when using a Siteimprove managed device (work laptop) and a Siteimprove approved connection to Siteimprove systems (VPN). Alternatives are not allowed nor technically possible.

1.16. Logging

Logging is used to troubleshoot and monitor Siteimprove systems for abnormal functional patterns, suspicious behaviour and other activities incompliant with the existing legislation and Information Security policy. Customer data access logs are reviewed as part of an incident and as part of the annual Internal Security Audit.

Logs are centralized into separate information systems, which only staff with a relevant business need has access to, and is limited to staff from Information Security, IT support, IT infrastructure, Operations and Development departments. Logs are kept for as long as needed from a business perspective.

1.17. Data collection and cookies

When it comes to Siteimprove Analytics, Siteimprove collects customer website visitor analytics data via the script on your website, which passes information through our endpoints to datacenters. These endpoints are located based on customer location so that collection is done more efficiently.

To make website and other communications related to Siteimprove services work properly, we place small text files (cookies) on your device when you visit our website. For more information about usage of cookies, please visit https://support.siteimprove.com/hc/en-gb/articles/115000070092-Analytics-Technical-Specifications

1.18. CCPA compliance

Siteimprove is committed to CCPA compliance in both its own internal processing of Personal Information as well as customer-use of the Siteimprove Intelligence Platform. For further information on this matter please visit Siteimprove's Privacy and Security webpage.

1.19. Regular testing and evaluation of the effectiveness of the technical and organizational security measures

Internal security audit

In order to properly implement the Siteimprove Information Security policy, the Internal Security Audit is conducted every year, with the objectives of (1) assuring adherence to the Information Security Policy and other underlying policies, (2) monitor and follow-up on regulatory information security requirements relevant to Siteimprove (e.g. Personal Information processing), (3) Identify new risks and (4) Indirectly raise 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 the technical and organizational security measures.

Financial audit

Due to financial regulatory requirements, Siteimprove undergoes a Financial audit on a yearly basis. The IT infrastructure related to the financial data processing is included in the audit and servers as an additional, external, objective method of assessing and evaluating the effectiveness of the technical and organizational security measures.

Penetration testing and vulnerability management

To continuously assure a reliable and secure product for Customers, Siteimprove has its application suite tested for security vulnerabilities, both internally and externally.

- Internally, this is done through quality checks before each release as well as 'bug hunting' sessions, where Siteimprove's developers will try out new features to discover if the application is not responding as it should.
- Externally, this is done annually by a 3rd party entity that specializes in penetration testing services which performs an annual assessment of OWASP top 25 vulnerabilities.

The process concludes with a vulnerability report which serves as input for the development of the application. Siteimprove, as with any other software developer company or cloud provider, cannot fully guarantee the lack of specific vulnerabilities due to the nature of the field – but Siteimprove does apply a reasonable amount of effort to prevent, identify and remediate vulnerabilities.

Code development and review

We follow Agile development methodology which help us to provide a quick and proper answer to any feedback given by our customers or internal quality assurance tests, assessing continuously the direction of the project during its development cycle. Our code runs through multiple individual (unit testing), automated (multiple tests in the CI/CD pipeline) and manual tests (through internal peer-review) and transitions through the development and staging environments, before being deployed to production.

Reviews of Security Documentation

After the parties have entered into 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 ISO 22301 Certification
- the then-current SOC 2 Report for Siteimprove infrastructure providers
- the then-current Penetration testing attestation for the Siteimprove Intelligence Platform
- the Siteimprove Business Continuity Plan
- the Siteimprove Master Disaster Recovery Plan

1.20. References

- https://siteimprove.com/en/privacy/
- https://siteimprove.com/en/privacy/data-breach-policy/
- https://siteimprove.com/en/privacy/vulnerability/
- https://siteimprove.com/en/privacy/information-security-notice/
- https://siteimprove.com/en/privacy/privacy-policy/
- https://siteimprove.com/en/privacy/website-privacy-policy/

Siteimprove

Appendix 2 – Information about locations for processing and sub-suppliers (sub-processors)

This Appendix constitutes Siteimprove's disclosure to Customer of sub-processors used to provide the Included Services. It is an integrated part of the CCPA DPA and its inclusion consititutes Customer's agreement to the use of said sub-processors.

2.1 Interxion

Interxion is the primary hosting location for the Siteimprove infrastructure, from which 99.9% of Siteimprove customers receive their service. Interxion is located in Industriparken 20A DK, 2750 Ballerup, Denmark - just outside Copenhagen. This location contains the bulk of the Siteimprove application logic and the various database back-ends. Only a limited number of named Siteimprove employees have physical access to the data center.

Interxion is a state-of-the-art data center provider with:

- Power delivery with 99.999% SLA
- Temperature and humidity is monitored 24x7 and is in line with ASHRAE recommendations
- Diverse ISP connectivity
- A very early smoke detection system is installed with direct lines to fire stations
- Automatic gas-based fire suppression systems
- Fire-retardant walls
- Trained security staff on site 24x7
- Five layers of physical security
- Access tokens in combination with biometric data and mantraps are used for data center entry
- CCTV video surveillance

Interxion has access procedures in place for personnel and goods entry and maintains an access log for all entry to the data center.

Interxion is a ISO 27001:2013(Information Security) and ISO 22301:2012(business continuity) certified data center provider. Interxion does also undergo a yearly SOC2 audit. Both the certificates and the audit report can be provided to customers, upon request.

Further information about Interxion can be found on their website at
www.interxion.com/locations/denmark/copenhagen/

2.2 Amazon Web Services (AWS)

The AWS region in Frankfurt, Germany is utilized by Siteimprove for storage of PDF files collected by the Quality Assurance service and storage of Response website snapshots.

AWS is also used for off-loading application servers located in Interxion. When certain thresholds are met, workloads are moved to AWS for processing, after which, the processed data is returned to Interxion.

AWS is considered one of the top providers of cloud services and hold a number of certifications and are on a yearly basis subjected to several independent audits in order to maintain the certifications.

AWS website: https://aws.amazon.com/compliance/

Siteimprove

Appendix 3 – Instructions

3.1 Instructions

The Customer hereby instructs the Supplier to process the Customer's Personal Information for use for operation and maintenance of the Customer's website and to form an overview of the website traffic; see the Service Agreement.

If the Supplier leaves the processing of the Customer's Personal Information to sub-processors, the Supplier is responsible for entering into written data (sub-)processing agreements with these; see Clause 5.3. The Supplier is responsible for ensuring that the Customer's instructions are sent to any sub-processors.

3.2 Purpose of the processing

The Supplier is a multinational software-as-a-service provider which gives customers access to cloud-based tools and services that automate the process of identifying errors, faults and deficiencies on websites. The Supplier's Intelligence Platform constitutes a collection of integrated tools for management and optimization of website content, improvement of search engine optimization (SEO), monitoring of website performance and/or use of website analysis data. The Customer has purchased access to such services.

3.3 General description of the processing and type of Personal Information

The Supplier'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, the Supplier collects and processes both personally attributable and not personally attributable data on the Customer's website in connection with the provision of the services. The data processing may include Personal Information and any other identifier which is present on the website on which Siteimprove services are being used. The categories of Personal Information collected through the Siteimprove Intelligence Platform depend on the content of the websites but will only include processing of ordinary Personal Information, such as name, e-mail address, telephone number, job position etc. If using Siteimprove Analytics, IP addresses of visitors to the Customer's website will also be processed, whereas the Customer can limit such processing by setting IP anonymization as standard. Through the services, the Supplier does not seek to collect any sensitive Personal Information subject to heightened regulations (e.g. HIPAA, FERPA). The Supplier does not sell the processed data to a third party.

3.4 Categories of Consumers

Personal Information are processed about the following categories of Consumers:

A) Any person who may be stated or identifiable on the Customer's website.

Site Improve 03092022

APPROVED AS TO FORM:

Kimberly Colliot Wesley
Criminal District Attorney's Office*

CERTIFICATION OF
AVAILABLE FUNDS: $_____

_____
Tarrant County Auditor

*By law, the Criminal District Attorney's Office may only approve contracts for its clients. We reviewed this document as to form from our client's legal perspective. Other parties may not rely on this approval. Instead those parties should seek contract review from independent counsel.