# SiteimproveData Processing Agreement

**Salesforce Quote:**

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

|  |  |
| --- | --- |
| **Entity:**    **Address:**    **Company reg. no:**    (“**the Customer**”) | **Entity:**  Siteimprove A/S  **Address:**  Sankt Annæ Plads 28 1250 København K Denmark  **Company reg. no:**  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:

# General terms

* 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 **Master Subscription Agreement**”). The Data Processing Agreement will take precedence over any corresponding or conflicting provisions in the Master Subscription Agreement and any other contractual documents.
  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.
  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.

# The Customer’s rights and obligations

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

# The Supplier’s Obligations

* 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.
  2. The Supplier only processes received personal data in accordance with documented instructions from the Customer (see clause 4 Instructions and Appendix 3 – Instructions) and solely for the performance of the Master Subscription Agreement.
  3. The Supplier must continuously keep a record of the processing of personal data as well as a record of all personal data breaches. The Supplier shall assist the data controller in notifying the personal data breach to the competent supervisory authority, pursuant to Article 33(3) GDPR. Following shall be stated in the Supplier’s notification to the competent supervisory authority:
  4. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
  5. the likely consequences of the personal data breach;
  6. the measures taken or proposed to be taken by the Supplier to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
  7. 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 - Description of the technical and organizational security measures implemented.
  8. 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 data subjects about access to their own data, disclosure of the data subject’s data, rectification and erasure of data, restriction of processing of the data subject’s data, as well as the Customer’s obligations in relation to notification of the data subject in the event of personal data breaches.
  9. The Supplier must assist the Customer in compliance with the Customer’s obligations under Articles 32-36 of the General Data Protection Regulation.
  10. 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.

# Instructions

* 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-processors) receive the Customer’s instructions; see Appendix 3 – Instructions.
  2. The Supplier must notify the Customer immediately if the Supplier finds that an instruction is contrary to the General Data Protection Regulation.

# Sub-processors

* 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.
  2. The Supplier must not, without the Customer’s express written approval, use sub-processors other than those specified in Annex 2 – Sub-processors, including replacement of these sub-processors, for processing of the personal data which the Customer has instructed the Supplier to process pursuant to the Master Subscription Agreement. The Customer cannot refuse to approve the addition or replacement of a sub-processor unless there are specific, reasonable grounds.
  3. The data sub-processing agreement must impose on the sub-processor the same data protection obligations imposed on the Supplier under this 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.
  4. 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-processor’s compliance with their obligations; see clause 5.3 of the Agreement.
  5. 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.
  6. All communication between the Customer and the sub-processor will take place via the Supplier.

# Technical and organizational security measures

* 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:
     1. destruction, loss, alteration, or impairment,
     2. disclosure to unauthorized parties or unauthorized use or from other processing in contravention of the legislation; see clause 1.2 of the Agreement.
  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 - Description of the technical and organizational security measures implemented.
  3. The Supplier and its employees are prohibited from obtaining information of any kind which is not relevant to the performance of their tasks.
  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.
  5. The Supplier is obliged to notify the Customer of any personal data breach immediately after the occurrence thereof.
  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.

# Transfers to third countries

* 1. The Supplier shall ensure that the personal data is stored within the EU / EEA by an organization established within the EU / EEA, unless the parties have agreed otherwise.
  2. The Supplier will only transfer personal data to third countries if instructed by the Customer; see Appendix 3 – Instructions.
  3. In connection with transfers to third countries, the Supplier and the Customer are jointly responsible for ensuring that there is a valid transfer basis.

# Duty of confidentiality

* 1. During the term of the Master Subscription 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.
  2. The Supplier must ensure that anyone who is authorized to process personal data covered by the Agreement, including employees and sub-processors, undertake a duty of confidentiality or are subject to an appropriate statutory duty of confidentiality.

# Checks and declarations

* 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.
  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 Master Subscription Agreement.
  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 Master Subscription Agreement, secondarily in a separate agreement between the parties if the scope and process are not covered by the Master Service Agreement. The Customer’s costs for the inspection are payable by the Customer.
  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.

# Erasure of data

* 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 Master Subscription Agreement.
  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.
  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.

# Amendments to the Agreement

* 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 Master Subscription Agreement, pricing must be agreed before the amendments take effect.
  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.

# Governing law

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

# Commencement and term

* 1. The Agreement is entered into when signed by both parties and will run until the termination of the Master Subscription 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:  **Signature**  **Name**  Richard Reynolds  **Position**  Director, Security  **Date**  **July 6, 2022** | On behalf of Customer:  **Signature**  **Name**  **Position**  **Date**  **July 6, 2022** |

**Appendices:**

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

**Appendix 2 – Sub-processors**

**Appendix 3 – Instructions**

# Appendix 1 - Description of the technical and organizational security measures implemented

## Security measures in general

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.

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 an organisational unit comprised of three teams: Security Operations, Information Assurance and Governance, Risk and Compliance. Siteimprove has appointed a Director of Security role to lead this function, which reports to the Chief Information Officer. Specific details about the points in this Appendix can be found under References in section 22.

## 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 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 sub-processors 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.

## Security contact

The single point of contact for Siteimprove security matters is the Siteimprove Information Security team: [security@siteimprove.com](mailto:security@siteimprove.com).

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.

## 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 are 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 an internal security audit.

## Security incidents

* 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.
  2. Examples of security incidents include:
     1. Virus/ransomware infection
     2. Suspicious activity on company devices or accounts
     3. Former employee suspected of accessing Siteimprove network or tools after contract termination.
  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:
     1. Critical - related to critical assets or situations that can lead to a disaster.
        1. Handling: As soon as possible following notification/identification and solved as soon as possible
        2. Example: Ransomware infection on multiple subnets with a big probability to infect development or production servers
     2. High - related to important assets or situations that can lead to a disaster.
        1. Handling: Within two (2) hours of notification/identification and solved as soon as possible
        2. Example: Ransomware infection on an isolated network segment
     3. Medium - related to generic assets and situations affecting multiple users.
        1. Handling: Within one (1) business day and solved within seven (7) business days
        2. Example: Multiple user endpoints infected with adware
     4. Low - related to generic assets and situation affecting one user.
        1. Handling: Within three (3) business days and solved within ten (10) business days
        2. Example: User endpoint infection with adware
  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:
     1. Preparation
     2. Identification
     3. Containment
     4. Investigation
     5. Eradication
     6. Recovery
     7. Reporting
     8. Lessons learned
  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](mailto:status@siteimprove.com) as well.

## Pseudonymization and encryption

Siteimprove assures the confidentiality and integrity of personal data 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).

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.

## Data retention and backup

* 1. Siteimprove will store personal data provided by the Customer:
     1. As long as the Agreement between Siteimprove and Customer stands, we process and retain the personal data provided by the Customer.
     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.
  2. However, Siteimprove will retain some information about the Customer after the contract termination, due to legal and financial requirements.
  3. When the Agreement between Siteimprove and Customer is terminated, the following will happen:
     1. The tables in the database, containing the customer results, history, and specific customizations to the Siteimprove Suite will be dropped.
     2. Crawled website data (HTML) and/or any linked documents (such as PDF files) will be deleted.
     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 ninety (90) days after initiation.
  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.
  5. Personal data belonging to Customers within the EU will be stored, processed, and backed up in the EU components of the Siteimprove infrastructure.

## Physical security

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

## Interxion

Interxion is an 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.

Further information about Interxion security posture can be found on their [official website](https://www.interxion.com/Locations/copenhagen/).

## 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](https://aws.amazon.com/security/).

## Siteimprove’s access to personal data provided by the Customer

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.

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](https://pages.nist.gov/800-63-3/sp800-63-3.html)), including an annual review of users in order to check correct operations. Multifactor authentication is implemented wherever technically feasible.

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.

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).

## 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](https://support.siteimprove.com/hc/en-gb/articles/207430923-User-Roles-Rights). 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](https://support.siteimprove.com/hc/en-gb/articles/115000253291-Password-Policy-Frequently-Asked-Questions). There is also a possibility to create additional user roles.

Regarding authentication, the platform uses its own repository of users with local authentication. It is possible to configure Single Sign On (SSO) depending on the selection of Siteimprove’s [Technical Support Schemes available](https://siteimprove.com/en-us/services/support/). Session hijacking is prevented by encryption in transit of the session, applying the "secure" flag to the session cookie.

## 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.

## Network and host protection

To ensure the 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.

## 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.

## 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: (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.

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](https://status.siteimprove.com/)

Siteimprove maintains business impact assessments to determine its 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.

## 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.

## Logging

All Siteimprove infrastructure and applications are monitored by the 24 by 7 Security Operations function to detect and respond to suspicious behaviour. This is supported by the Information Assurance & GRC functions which deliver risk management, compliance and audit.

Logs are used by operational and development teams to troubleshoot service delivery issues. Role based access control is applied to restrict staff from support functions to the data required to fulfil their role.

## 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 the website and other communications related to Siteimprove services work properly, we place small text files (cookies) on the website visitor’s device. For more information about the usage of cookies, please visit <https://support.siteimprove.com/hc/en-gb/articles/115000070092-Analytics-Technical-Specifications>.

## GDPR compliance

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 [Privacy and Security webpage](https://www.siteimprove.com/privacy/).

## 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 (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.

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.

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.
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.
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.

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:

1. the certificates issued for Siteimprove infrastructure providers in relation to the ISO 27001 Certification, the ISO 22301 Certification.
2. the then-current SOC 2 Report for Siteimprove infrastructure providers.
3. the then-current Penetration testing attestation for the Siteimprove Intelligence Platform.
4. the Siteimprove Business Continuity Plan.
5. the Siteimprove Master Disaster Recovery Plan.

## References

[**https://siteimprove.com/en/privacy/**](https://siteimprove.com/en/privacy/)

# Appendix 2 – Sub-processors

This Appendix constitutes Siteimprove’s disclosure 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.

| **Company name** | **Company information** | **Location and description of processing** |
| --- | --- | --- |
| **InterXion** | **Company registration number:**  25147022  **Registered office**:  Industriparken 20A,  2750 Ballerup, Denmark | **Denmark, Ballerup**  Primary hosting location for the Siteimprove infrastructure. This location contains the bulk of the Siteimprove application logic and the various database back-ends. |
| **Amazon Web Services EMEA SARL (AWS)** | **Company registration number**:  B-93815  **Registered office:**  38, Avenue John F. Kennedy,  L-1855 Luxembourg  **AWS entity**: A100 ROW GmbH | **Frankfurt, Germany**  Hosting location for some of our service components, which mainly relates to the storage of crawled content from Customers’ websites by the Quality Assurance service. |

# Appendix 3 – Instructions

1. Instructions

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 [Master Subscription Agreement](https://www.siteimprove.com/legal/master-subscription-agreement/).

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 5.3. The Supplier is responsible for ensuring that the Customer’s instructions are sent to any sub-processors.

1. 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.

1. General description of data processing

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 technically necessary. After collection of IP addresses, they will be anonymized and thereby not traceable in the Siteimprove Intelligence Platform.

1. Type of Personal data

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

1. Categories of data subjects

Data are processed about the following categories of data subjects (e.g., citizens, students, employees etc.): Any person who may be stated or identifiable on the Customer’s website.

1. Third countries (non-EU member states)

The Supplier does not conduct transfers personal data to third countries as part of the provision of the Supplier’s services.