Privacy Notice

Last Updated: May 24, 2018
Effective as of: May 25, 2018

Introduction

Area 1 Security ("Area 1") values privacy, security, and trust as paramount in the relationships we have established and will establish with our customers, partners and employees. Our customers, partners, and employees may provide us access to certain data to help us operate, improve or enhance our services ("Services"). The following describes our philosophy with respect to data we collect and use as part of providing our Services and fulfilling our mission of eliminating the threat of online phishing attacks.

When we talk about "Area 1," "we," "our," or "us," in this notice, we are referring to Area 1 Security, Inc. When we say "you" or "End-User" in this notice, we mean any individual using and accessing our Services. When we talk about an "Organization" or "Customer" in this Notice, we are generally referring to the entity of which you are an employee, contractor, member, or other participant, that has engaged us to provide the services under the terms of a contract.
By sharing your personal information with us, and by continuing to use our Services, you confirm that you have read and understood the terms of this Notice.

When you apply for a role with Area 1 through our Website or otherwise, please see our Candidate Privacy Notice (forthcoming as of May 25, 2018).

If you have any questions, comments or concerns about any aspect of this Notice or how we handle your information, please reach out to our team using the details provided under the "Contact Us" section of this Notice.

Privacy Principles

Trust and transparency are foundational to what we do at Area 1. We are committed to being open about how we approach privacy at Area 1 and aim to communicate with you about privacy in a way that is easy for you to understand. To support these goals, we developed these Privacy Principles to highlight our commitment to responsibly protecting and handling your personal information. Our Privacy Principles help guide decisions we make at every level of our organization, every day so that we can fulfill our mission to provide security in a way that is consistent with our core values as well as our legal obligations.

Our core Privacy Principles are:

1. **Integrity**. We do not sell data.
2. **Transparency**. We are transparent with our customers, partners and employees about how we collect, use and share data.

3. **Security**. Security is both our business and highest priority. We use standard best practices and advanced organizational, technical, and behavioral security measures to protect data.
4. **Minimal Collection**. We are not in the business of collecting personally identifiable information. We leverage data to operate and enhance our Services for our customers. Personally Identifiable Information (PII) that may be associated with the data we use is incidental.
5. **Accountability**. We take the protection of data very seriously.

Notice to End Users

In general, our Services are intended for use by Organizations, administered to you by your Organization, and subject to your Organization's policies, if any. This means that in most cases we are collecting and processing your personal information on behalf of your Organization. In these cases, we are generally acting as a processor of your personal information, processing the information according to your Organization's instructions, because your Organization is the controller. It is primarily your Organization, as the controller, that controls what personal information about you we collect and how we use it. If you have privacy-related questions or concerns about your Organization's privacy practices or the choices your Organization has made to share your information with us or any other third party, you should reach out to your Organization's Administrator or see your Organization's privacy policies. Area 1 is not responsible for the privacy or security practices of our Customers, which may differ from those set forth in this Notice.

Quick links

We encourage you to read this entire Notice carefully to help ensure you are fully informed about privacy as it relates to our Services. However, if you only want details about a specific privacy practice of ours, we have provided easy-to-navigate links that you can use to quickly jump to the relevant section of this Notice.

Who we are

What information we collect and how

How we use the information we collect

Who we share your personal information with

Cookies and similar technologies

How we keep your personal information secure

International data transfers

Data retention

Legal basis for processing (European Economic Area users only)

Your rights, controls, and choices

How does our site handle Do Not Track signals

No information collected from children

Fair Information Practices

Changes to this Privacy Notice

Contact Us

Who we are
Area 1 is a performance-based cybersecurity company providing solutions to help businesses protect against phishing attacks. Find out more here.

Area 1 Security, Inc. is a company incorporated under the laws of the State of Delaware, USA and whose principal office is located at 142 Stambaugh Street, Redwood City, CA 94063.

What personal information we collect and how
We know that personal information is defined slightly differently across the world. That said, at Area 1, we define it as any information that could be used to identify you or another individual. We think that this broad definition enables us to better respect your privacy and safeguard the information entrusted to us.

The personal information that we collect about you broadly falls into two categories - information that is provided to us, and information we process on behalf of your Organization.

Information that is provided to us

Public Forums: We collect other information, including Personal Information that you submit to our Website or as you participate in certain interactive features of our Services. You should be aware that any information (including Personal Information) you provide in these areas may be read, collected, and used by others who access them. To request removal of your Personal Information from our blog or community forum, contact us at privacy@area1security.com. In some cases, we may not be able to remove your Personal Information, in which case we will let you know if we are unable to do so and why.

Social Media Widgets: Our website includes plugins for social media platforms, such as facebook.com of Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA; Twitter.com of Twitter Inc., 795 Folsom St., Suite 600, San Francisco CA 94107, USA; and Google+ of Google Inc., 1600 Amphitheatre Parkway Mountain View, California, 94043, USA. Social Media Features and Widgets are either hosted by a third party or hosted directly on our websites.

You can generally identify the plugins by the respective network's logo, for instance in combination with a pictogram of a clenched hand with a raised thumb or the addition of a "recommendation", "like" or "comment."

Details about purpose and extent of data collection as well as processing and usage of the data by the social media networks can be obtained by reading the privacy policies of Facebook, Twitter, and Google.

Cookies and other Tracking Technologies

When you visit our Website or use our Services, we use "cookies" and other tracking technologies like "web beacons" to allow us to remember your user preferences, to maximize the performance of our Website and Services, enhance and personalize your experience and provide marketing communications. They also help ensure that advertisements you see while you are on our Website are more relevant to your interests.

You can choose to have your computer warn you each time a cookie is being sent, or you can choose to turn off all cookies. You do this through your browser settings. Since the browser is a little different, look at your browser's Help Menu to learn the correct way to modify your cookies.

If you turn cookies off, some of the features that make your site experience more efficient may not function properly. It won't affect the user's experience that makes your site experience more efficient and may not function properly.

Testimonials/Reviews/Feedback: We may post customer testimonials on our Website, which may contain Personal Information. We do obtain the customer's consent via email prior to posting the testimonial to post their name along with their testimonial. If you want your testimonial removed, please contact us at privacy@area1security.com.

Surveys: We may provide you the opportunity to participate in contests or surveys. If you participate, we will request and collect certain Personal Information from you at the time of the survey. Participation in these surveys or contests is completely voluntary and you have a choice whether or not to disclose this information. The requested information typically includes contact information, such as email or phone number.

Other Direct Contact: If you ever communicate directly with us, we will maintain a record of those communications and responses.

Organization Administrators: Your Organization's Administrator may provide personal information to us through the Services. We generally ask for more information about Organization Administrators in order to provide the Services and help manage the Organization's Account. We ask Organization Administrators to provide the following information about themselves:

Name
Email Address
Billing and Delivery Address
Telephone Number
Job Title
Organization Name
information about other Organization Administrators working on related projects

In addition, if you purchase our Services either as an Organization Administrator you will need to share payment and billing information such as your credit card details and billing address, and we will maintain a record of your purchases and transactional information.

Credit Card Information

Credit cards, debit cards or other means may be used to pay for our Services. We do not collect this credit card, debit card or personal financial account information. Instead, we use a third party service provider to process our subscription billing. If you provide payment information to pay for the Services, you provide it directly to our service provider and not to Area 1. You will automatically be routed to the third party website to provide the information the third party requires to process your transaction. This third-party vendor and has its own privacy statements. This Notice does not cover information collected by the third party vendor and Area 1 is not covered by or responsible for their privacy practices or statements.

Information we process on behalf of your Organization

When your Organization or your Organization Administrator upload, input or generate personal information in the Services about you (their End Users), we will typically act as a processor and process such personal information on behalf of your Organization and our privacy practices will be governed by the contract we have in place with your Organization. This Notice will not apply to such personal information.

How we use the information we collect

In general, we use the personal information we collect to operate our business and provide our Services, which includes using data to improve, research and develop our product offerings.

We may use the personal information we collect through the Services for a range of reasons, including:

- to provide and maintain the Services.
- to manage your Organization's account with us, including for billing purposes as well as for our customer relationship management.
- to personalize the Services and improve the experience.
- to improve our products, technology and Services, and, where agreed, to provide
- updates on how we are improving the Services based on any feedback.
  to analyze use of the Services in order to ensure the technical functionality of our

products, technology, and Services, and to research and develop new products and services.

- to conduct aggregate statistical analysis with "Performance Data.” Performance Data includes aggregate, de-identified usage information and other aggregate measures of the Services’ performance. We may share aggregated, de-identified Performance Data with third parties to help us better understand our customers’ needs and improve the Services.
- to prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, and criminal activity.
  to comply with and enforce applicable legal requirements, agreements, and policies.
  to perform other activities consistent with this Notice.

Who we share your personal information with

We do not sell, trade or otherwise transfer PII that could identify either a person or a customer to third parties as part of our Services. unless we provide users with advance notice. This does not include website hosting partners and other parties who assist us in operating our website, conducting our business, or serving our users, so long as those parties agree to keep this information confidential. If we leverage data from customers to create derivative works to operate or enhance our Services, we would sanitize those derivative works so that they would not identify any person or customer.

As noted above, we may share PII provided by a customer to that customer as part of operating our Services. We may also use and disclose PII as required to comply with a court order or applicable law. Non-personally identifiable visitor information may be provided to other parties for marketing, advertising, or other uses.

How we keep your personal information secure

Security is what we do, and we take the security of the personal information we have about you very seriously. We use appropriate administrative, organizational, technical and physical safeguards that are designed to protect the personal information we collect and process about you. The measures we use are designed to provide a level of security appropriate to the risk of processing your personal information and to help ensure that your data is safe, secure, and only available to you and to those with authorized access (as decided by your Organization Administrator or you, as appropriate). All of our employees undergo background checks prior to beginning employment. We also enforce access control and mandate role-based training for any employees requiring access to data that may contain PII.

International data transfers

We are headquartered in the United States and operate internationally. Therefore, you should be aware that we may transfer or process your personal information in countries other than the country in which you are a resident. These countries may have data protection laws that are

different than the laws of your country, and in some cases may not be as protective.

Specifically, our Website servers are located in the United States, and our third party service providers, including Amazon Web Services (“AWS”), Google Cloud Platform (“GCP”) and partners, operate in the United States and in other countries around the world. This means that when we collect your personal information we may process it in any number of places around the world.

Wherever, therefore, your personal information is transferred, stored or may be processed by us, we will take reasonable steps to safeguard the privacy of your personal information as indicated in this Notice. Additionally, when using or disclosing personal information transferred from outside the European Economic Area, we use and in countries which are not subject to an adequacy decision by the European Commission and which may not provide for the same level of data protection in the European Economic Area. In this event, we will ensure that such recipient offers an adequate level of protection, for instance by entering into standard contractual clauses for the transfer of data as approved by the European Commission, adopt other means under applicable law for ensuring adequate safeguards, or obtain your (Art. 46 GDPR), or we will ask you for your prior consent. to such international data transfers.

If you would like a copy of our standard contractual clauses or more information on the appropriate safeguards we have implemented with our third party service providers and partners, please reach out to us using the details provided under the “Contact Us” section of this Notice.

How long we keep your personal information
We only keep your personal information for as long as we have an ongoing legitimate business need to do so (for example, to fulfill the purposes outlined in this Notice, to provide the Services or to comply with legal, tax or accounting requirements, to enforce our agreements or to comply with our legal obligations).

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it. If this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

Legal basis for processing (European Economic Area users only)
If you are a user from the European Economic Area, where we are collecting your personal information as a processor on behalf of your Organization (the controller), our legal basis for doing so will depend on the personal information concerned and the specific context in which we collect it. However, as it relates to our Services, we will normally collect personal information from you only where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms, or where we need the personal information to perform a contract with your Organization..

If we ask you to provide personal Information to comply with a legal requirement or to enter into a contract, we will make this clear at the relevant time and let you know if the personal information is mandatory or not (as well the possible consequences if you do not provide it). Similarly, if we collect and use your personal information in reliance on our legitimate interests (or those of any third party) that are not referred to in this Notice, we will make it clear to you at the relevant time what those legitimate interests are. Typically, our legitimate interests include improving, maintaining, developing and enhancing our technology, products, services, ensuring the security of the Services and for our marketing purposes.

If you have questions or need further information about the legal basis we rely on to collect and use your personal information, please reach out to us using the details provided under the “Contact Us” section of this Notice.

Your rights, controls, and choices

As we noted in the “Notice to end users” section of this Notice, for all of the personal information we collect and process through the Services, Area 1 Security acts as a processor for its Customers, the Organization. You have certain rights regarding your personal information, subject to applicable data protection laws, including the following:

- to access your personal information held by us (right to access);
- to rectify inaccurate personal information and ensure it is complete (right to rectification);
- to erase/delete your personal information to the extent permitted by other legal obligations (right to erasure; right to be forgotten);
- to restrict our processing of your personal information (right to the restriction of processing);
- to transfer your personal information to another controller to the extent possible (right to data portability);
- to object to any processing of your personal information carried out on the basis of our legitimate interests (right to object). Where we process your personal information for direct marketing purposes or share it with third parties for their own direct marketing purposes, you can exercise your right to object at any time to such processing without having to provide any specific reason for such objection;
- not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects ("Automated Decision-Making"); Automated Decision-Making currently does not take place on our websites;
- to the extent we base the collection, processing and sharing of your personal information on your consent, to withdraw your consent at any time, without affecting the lawfulness of the processing based on such consent before its withdrawal.

If you would like to exercise data protection rights for this personal information – including your rights to access, correct, or delete such data – you should contact your Organization directly

and it will deal with your request. Where required, we may provide assistance to the Organization.

You can opt out of receiving promotional emails or text messages from us by clicking the “unsubscribe” link in the email or by emailing privacy@area1security.com.

How does our site handle Do Not Track signals?
We honor Do Not Track signals and Do Not Track, plant cookies, or use advertising when a Do Not Track (DNT) browser mechanism is in place. It's also important to note that we allow third-party behavioral tracking.

Children’s information
When it comes to the collection of personal information from children under the age of 13 years old, the Children's Online Privacy Protection Act (COPPA) puts parents in control. The Federal Trade Commission, United States' consumer protection agency, enforces the COPPA Rule, which spells out what operators of websites and online services must do to protect children's privacy and safety online. We do not knowingly collect or store any personal information from anyone under 13 years of age. The Services are directed to businesses and users who are at least 18. If you are under the age of 18, you may not use the Services.

Changes to this Privacy Notice
From time to time, we may change this Privacy Notice in response to changing technologies, industry practices, and regulatory requirements or for other purposes. We will provide notice to you if these changes are material (this notice may be by email to your Organization’s Administrator or you at the last email provided us, by posting notice of such changes on the Website, or by other means, consistent with applicable law) and, if required by applicable law, we will obtain your consent.

You can see when this Notice was last updated by checking the “last updated” date displayed at the top of this Notice.

Fair Information Practices
The Fair Information Practices Principles form the backbone of privacy law in the United States and the concepts they include have played a significant role in the development of data protection laws around the globe. Understanding the Fair Information Practice Principles and how they should be implemented is critical to comply with the various privacy laws that protect personal information.

In order to be in line with Fair Information Practices we will take the following responsive action, should a data breach occur:

We will notify you via email
- Within 7 business days

We will notify the users via in-site notification

- Within 1 business day

We also agree to the Individual Redress Principle which requires that individuals have the right to legally pursue enforceable rights against data collectors and processors who fail to adhere to the law. This principle requires not only that individuals have enforceable rights against data users, but also that individuals have recourse to courts or government agencies to investigate and/or prosecute non-compliance by data processors.

Contact Us

We encourage you to contact us if you have any comments or questions about this Privacy Notice or our related privacy practices. You may reach us at privacy@area1security.com or at our mailing address below:

Area 1 Security, Inc.
Privacy Department
142 Stambaugh Street
Redwood City, CA 94063
privacy@area1security.com

If you are resident in the EEA, the controller of your personal information is the underlying organization that is a customer of Area 1 Security.