

Ensignten Privacy Policy

PART I. GENERAL INFORMATION

Our commitment to privacy

Your privacy is important to us and maintaining your trust is our priority. To ensure that your privacy is protected and your privacy choices are respected, we have set out in this Privacy Policy an explanation of our online information practices as well as the decisions you may make regarding how your information is collected and used when viewing our websites and their sub-domains (the “Websites”). We also describe in this Privacy Policy how we collect and use information in the course of providing tag management and data intelligence services (the “Ensignten Services”) to our customers. As used herein, “Services” means the Websites and the Ensignten Services.

Remember that your use of our Services is at all times subject to our [Terms of Use](#), which incorporate this Privacy Policy. Any terms we use in this Policy without defining them have the definitions given to them in the Terms of Use.

If you have a disability, you may access this Privacy Policy in an alternative format by contacting privacy-rights@ensighten.com.

PART II. WHAT WE COLLECT AND HOW WE USE IT

Categories of Personal Data We Collect

The following subsections detail the categories of Personal Data that we collect and have collected over the past twelve (12) months. “Personal Data” means any information that identifies or relates to a particular individual and also includes information referred to as “personally identifiable information” or “personal information” under applicable data privacy laws, rules or regulations. For each category of Personal Data, these subsections also set out the source of that Personal Data, our commercial or business purpose for collecting that Personal Data and the categories of third parties with whom we share that Personal Data. More information regarding those sources and categories are set forth below.

<u>Category of Personal Data</u>	<u>Examples of Personal Data We Collect</u>	<u>Categories of Third Parties With Whom We Share this Personal Data:</u>
Personal Identifiers	<ul style="list-style-type: none">■ First and last name■ Email■ Phone number■ Job Title■ Company Name■ Country	<ul style="list-style-type: none">■ Service Providers■ Advertising Partners■ Business Partners■ Parties You Authorize, Access or Authenticate

Device/IP Data	<ul style="list-style-type: none"> ■ IP address ■ Device ID ■ Domain server ■ Type of device/operating system/browser used to access the Services 	<ul style="list-style-type: none"> ■ Service Providers ■ Advertising Partners ■ Business Partners ■ Parties You Authorize, Access or Authenticate
Web Analytics	<ul style="list-style-type: none"> ■ Web page interactions ■ Referring webpage/source through which you accessed the Services ■ Non-identifiable request IDs ■ Statistics associated with the interaction between device or browser and the Services 	<ul style="list-style-type: none"> ■ Service Providers ■ Advertising Partners ■ Business Partners ■ Parties You Authorize, Access or Authenticate
Other Identifying Information that You Voluntarily Choose to Provide	<ul style="list-style-type: none"> ■ Identifying information in emails or letters you send us (including via our “Contact Us” open text message form 	<ul style="list-style-type: none"> ■ Service Providers ■ Advertising Partners ■ Business Partners ■ Parties You Authorize, Access or Authenticate
Professional or Employment-Related Data	<ul style="list-style-type: none"> ■ Job Title ■ Company Name 	<ul style="list-style-type: none"> ■ Service Providers ■ Advertising Partners ■ Business Partners ■ Parties You Authorize, Access or Authenticate
Geolocation Data	<ul style="list-style-type: none"> ■ IP-address-based location information 	<ul style="list-style-type: none"> ■ Service Providers ■ Advertising Partners ■ Business Partners ■ Parties You Authorize, Access or Authenticate
Other	<ul style="list-style-type: none"> ■ Other personal information you choose to provide to us 	<ul style="list-style-type: none"> ■ Service Providers ■ Advertising Partners ■ Business Partners ■ Parties You Authorize, Access or Authenticate

Tracking Tools, Advertising and Opt-Out

The Services use cookies and similar technologies such as pixel tags, web beacons, clear GIFs and JavaScript (collectively, “Cookies”) to enable our servers to recognize your web browser and tell us how and when you visit and use our Services, to analyze trends, learn about our user base and operate and improve our Services. Cookies are small pieces of data– usually text files – placed on your computer, tablet, phone or similar device when you use that device to access our Services. We may also supplement the information we collect from you with information received from third parties, including third parties that have placed their own Cookies on your device(s). Please note that because of our use of Cookies, the Services do not support “Do Not Track” requests sent from a browser at this time. To find out more about “Do Not Track,” please visit <http://www.allaboutdnt.com>.

Our Websites use cookies (small text files containing a string of alphanumeric characters that we put on your computer) to distinguish you from other users of our Websites. For more information about our use of cookies, please see our [Cookie Policy](#).

What we collect from customers of Ensignten Services

If you are an Ensignten customer, then when your users access their data via our secure web interface, we collect certain device-related information about the way they use the Ensignten Services, such as their IP address, the type of browser they are using, and the numbers and durations of site visits. We also collect user ID, username, and password.

We use the information that we collect to deliver and improve the Ensignten Services, to relay administrative information, and to verify login information.

What we collect for customers when they use the Ensignten Services

When you use websites owned or controlled by our customers that are using Ensignten Services, you may also be providing certain additional types of information to our customers other than those described above, such as tracking tags and cookies, or any data that our customers choose to collect, store and use.

By default, the Ensignten Services do not collect, store or use any directly-identifying information, such as names or addresses. In fact, we recommend and encourage our customers not to collect, store or use any such directly-identifying personal information in connection with the Ensignten Services.

However, the Ensignten Services will collect certain information about your device. In this context, we collect only the device-related information that our customers instruct us to collect as necessary to provide the Ensignten Services to them. In general, this will typically include certain network-related information, the device’s hardware model, operating system version, and browser type and version. We use this information to help our customers understand the general locale of their visitors, to provide analytics information to our customers about how visitors interact with their digital properties and to monitor, maintain, and improve the Ensignten Services. We encourage our customers to disclose the use of the Ensignten Services in their own privacy statements.

In all cases, whether and what personal information is collected, stored or used will ultimately depend upon the individual privacy practices of the customer website you visit. You should always check the individual privacy policy of each website you visit before providing any information. If you have any questions about how our customers collect, store or use your information, you should contact them directly.

Categories of Sources of Personal Data

We collect Personal Data about you from the following categories of sources:

- **You**
 - When you provide such information directly to us.
 - When you create an account or use our Services.
 - When you voluntarily provide information in free-form text boxes through the Services or Website (e.g., in the “Contact Us” form) or through responses to surveys or questionnaires.
 - When you send us an email or otherwise contact us
 - When you use the Services and such information is collected automatically.
 - Through Cookies (defined in the “Tracking Tools, Advertising and Opt-Out” section below).
 - If you download and install certain software we make available, we may receive and collect information transmitted from your computing device for the purpose of providing you the relevant Services, such as information regarding when you are logged on and available to receive updates or alert notices.
- **Third Parties**
 - Vendors
 - We may use analytics providers to analyze how you interact and engage with the Services, or third parties may help us provide you with customer support.
 - We may use vendors to obtain information to generate leads and create user profiles.
 - If you attend one of our events, we may receive personal information about you from our event partners.
 - Advertising Partners
 - We receive information about you from some of our vendors who assist us with marketing or promotional services related to how you interact with our websites, applications, products, Services, advertisements or communications.
- **Our Commercial or Business Purposes for Collecting Personal Data**
- **Providing, Customizing and Improving the Services**
 - Creating and managing your account.
 - Processing orders or other transactions; billing.
 - Providing you with the products, services or information you request.
 - Meeting or fulfilling the reason you provided the information to us.
 - Providing support and assistance for the Services.
 - Improving the Services, including testing, troubleshooting, research, statistical and survey purposes, data analytics and product development.
 - Personalizing the Services, website content and communications based on your preferences.
 - Doing fraud protection, security and debugging.
 - Carrying out other business purposes stated when collecting your Personal Data or as otherwise set forth in applicable data privacy laws, such as the California Consumer Privacy Act (the “CCPA”) and the EU General Data Protection Regulation (the “GDPR”).
- **Marketing the Services**
 - Marketing and selling the Services.

- **Corresponding with You**
 - Responding to correspondence that we receive from you (including when you submit a request through the “Contact Us” form), contacting you when necessary or requested, and sending you information about our Services.
 - Sending emails and other communications according to your preferences or that display content that we think will interest you.
- **Meeting Legal Requirements and Enforcing Legal Terms**
 - Fulfilling our legal obligations under applicable law, regulation, court order or other legal process, such as preventing, detecting and investigating security incidents and potentially illegal or prohibited activities.
 - Protecting the rights, property or safety of you, Ensignten or another party.
 - Enforcing any agreements with you.
 - Responding to claims that any posting or other content violates third-party rights.
 - Resolving disputes.

We will not collect additional categories of Personal Data or use the Personal Data we collected for materially different, unrelated or incompatible purposes without providing you notice.

How We Share Your Personal Data

We disclose your Personal Data to the categories of service providers and other parties listed in this section. Depending on state laws that may be applicable to you, some of these disclosures may constitute a “sale” of your Personal Data. For more information, please refer to the state-specific sections below.

- **Service Providers.** These parties help us provide the Services or perform business functions on our behalf. They include:
 - Hosting, technology and communication providers.
 - Security and fraud prevention consultants.
 - Analytics providers.
 - Support and customer service vendors.
- **Advertising Partners.** These parties help us market our services and provide you with other offers that may be of interest to you. They include:
 - Ad networks.
 - Marketing providers.
- **Business Partners.** These parties partner with us in offering various services. They include:
 - Businesses that you have a relationship with.
 - Companies that we partner with to offer joint promotional offers or opportunities.
- **Parties You Authorize, Access or Authenticate**
 - Third parties you access through the Services.
 - Other users.

Legal Obligations

We may share any Personal Data that we collect with third parties in conjunction with any of the activities set forth in the “Meeting Legal Requirements and Enforcing Legal Terms” section above.

Business Transfers

All of your Personal Data that we collect may be transferred to a third party if we undergo a merger, acquisition, bankruptcy or other transaction in which that third party assumes control of our business (in whole or in part). Should one of these events occur, we will make reasonable efforts to notify you before your information becomes subject to different privacy and security policies and practices.

Data that is Not Personal Data

We may create aggregated, de-identified or anonymized data from the Personal Data we collect, including by removing information that makes the data personally identifiable to a particular user. We may use such aggregated, de-identified or anonymized data and share it with third parties for our lawful business purposes, including to analyze, build and improve the Services and promote our business, provided that we will not share such data in a manner that could identify you.

Personal Data of Children

We do not knowingly collect or solicit Personal Data about children under 16 years of age; if you are a child under the age of 16, please do not attempt to use the Services or send us any Personal Data. If we learn we have collected Personal Data from a child under 16 years of age, we will delete that information as quickly as possible.

PART III. DATA SECURITY AND RETENTION

We use appropriate technical, organizational and administrative measures to protect any personal information we process about our visitors, our customers and their end users. Transmissions to and from secure areas of our Website are protected using TLS (Transport Layer Security) encryption.

However, please note that no Internet transmission can ever be guaranteed 100% secure, and so we encourage you to take care when disclosing personal information online and to use readily available tools, such as Internet firewalls, anti-virus and anti-spyware software, and similar technologies to protect yourself online.

We retain Personal Data about you for as long as you have an open account with us or as otherwise necessary to provide you with our Services. In some cases, we retain Personal Data for longer, if doing so is necessary to comply with our legal obligations, resolve disputes or collect fees owed, or is otherwise permitted or required by applicable law, rule or regulation. We may further retain information in an anonymous or aggregated form where that information would not identify you personally.

PART IV. YOUR PRIVACY RIGHTS

Update and Access to Your Information

We provide all visitors to our Websites with the opportunity to access, review, modify, and delete any personal information that has previously been provided. You can send an email to privacy-rights@ensighten.com. If you

make a request to access your personal information, we may charge you a fee subject to a maximum specified by applicable law.

If you wish to access, review, modify, and delete any personal information that any Ensignten customer has collected through the use of our Services, please contact that customer directly.

Unsubscribe from Our Mailing List

You may at any time ask us to remove you from any mailing list on which you previously asked us to include you by sending us an email at privacy-rights@ensighten.com, or by clicking “Unsubscribe” in any e-mail communications we send you.

California Resident Rights

If you are a California resident, you have the rights set forth in this section. Please see the “Exercising Your Rights” section below for instructions regarding how to exercise these rights. Please note that we may process Personal Data of our customers’ end users or employees in connection with our provision of certain services to our customers. If we are processing your Personal Data as a service provider, you should contact the entity that collected your Personal Data in the first instance to address your rights with respect to such data.

If there are any conflicts between this section and any other provision of this Privacy Policy and you are a California resident, the portion that is more protective of Personal Data shall control to the extent of such conflict. If you have any questions about this section or whether any of the following rights apply to you, please contact us at privacy-rights@ensighten.com.

Access

You have the right to request certain information about our collection and use of your Personal Data over the past 12 months. In response, we will provide you with the following information:

- The categories of Personal Data that we have collected about you.
- The categories of sources from which that Personal Data was collected.
- The business or commercial purpose for collecting or selling your Personal Data.
- The categories of third parties with whom we have shared your Personal Data.
- The specific pieces of Personal Data that we have collected about you.

If we have disclosed your Personal Data to any third parties for a business purpose over the past 12 months, we will identify the categories of Personal Data shared with each category of third-party recipient. If we have sold your Personal Data over the past 12 months, we will identify the categories of Personal Data sold to each category of third-party recipient.

Deletion

You have the right to request that we delete the Personal Data that we have collected about you. Under the CCPA, this right is subject to certain exceptions: for example, we may need to retain your Personal Data to provide you with the Services or complete a transaction or other action you have requested. If your deletion request is subject to one of these exceptions, we may deny your deletion request.

Exercising Your Rights

To exercise the rights described above, you must send us a request that (1) provides sufficient information to allow us to verify that you are either the person about whom we have collected Personal Data or are an agent

authorized by that person, and (2) describes your request in sufficient detail to allow us to understand, evaluate and respond to it. Each request that meets both of these criteria will be considered a “Valid Request.” We may not respond to requests that do not meet these criteria. We will only use Personal Data provided in a Valid Request to verify your identity and complete your request. You do not need an account to submit a Valid Request.

We will work to respond to your Valid Request within 45 days of receipt. We will not charge you a fee for making a Valid Request unless your Valid Request is excessive, repetitive or manifestly unfounded. If we determine that your Valid Request warrants a fee, we will notify you of the fee and explain that decision before completing your request.

You may submit a Valid Request using the following methods:

- Email us at: privacy-rights@ensighten.com
- Submit a form at this address: www.ensighten.com/privacy-webform

You may also authorize an agent (an “Authorized Agent”) to exercise your rights on your behalf. To do this, you must provide your Authorized Agent with written permission to exercise your rights on your behalf, and we may request a copy of this written permission from your Authorized Agent when they make a request on your behalf.

Personal Data Sales Opt-Out and Opt-In

In this section, we use the term ‘sell’ as it is defined in the CCPA. While we are not in the business of selling your Personal Data, like many companies online, we use services provided by Google, Facebook and other advertising companies that track website visitor activity, including through Cookies (as further described in our [Cookie Policy](#)). Under the CCPA, sharing your data through third party Cookies for online advertising may be considered a “sale” of information. You can opt out of these sales by following the instructions in this section. Based on the foregoing, we sell your Personal Data to the following categories of third parties: Ad Networks and Marketing providers.

Over the past 12 months, we have sold the following categories of your Personal Data to categories of third parties listed above:

- Personal Identifiers
- Device/IP Data
- Web Analytics
- Geolocation Data

You have the right to opt-out of the sale of your Personal Data. You can opt-out using the following methods:

- You can complete the online form found here: www.ensighten.com/privacy-webform
- Email us at privacy-rights@ensighten.com

We Will Not Discriminate Against You for Exercising Your Rights Under the CCPA

We will not discriminate against you for exercising your rights under the CCPA. We will not deny you our goods or services, charge you different prices or rates, or provide you a lower quality of goods and services if you exercise your rights under the CCPA.

Other California Resident Rights

Under California Civil Code Sections 1798.83-1798.84, California residents are entitled to contact us to prevent disclosure of Personal Data to third parties for such third parties' direct marketing purposes; in order to submit such a request, please contact us at privacy-rights@ensighten.com.

Other State Law Privacy Rights

Nevada Resident Rights

If you are a resident of Nevada, you have the right to opt-out of the sale of certain Personal Data to third parties who intend to license or sell that Personal Data. You can exercise this right by contacting us at privacy-rights@ensighten.com with the subject line "Nevada Do Not Sell Request" and providing us with your name and the email address associated with your account. Please note that we do not currently sell your Personal Data as sales are defined in Nevada Revised Statutes Chapter 603A.

EU Residents

If you are a resident of the European Union ("EU"), United Kingdom, Lichtenstein, Norway or Iceland, you may have additional rights under the EU General Data Protection Regulation (the "GDPR") with respect to your Personal Data, as outlined below.

For this section, we use the terms "Personal Data" and "processing" as they are defined in the GDPR, but "Personal Data" generally means information that can be used to individually identify a person, and "processing" generally covers actions that can be performed in connection with data such as collection, use, storage and disclosure. Ensignten, Inc. and its wholly owned subsidiary Tagman, Ltd will be the controllers of your Personal Data processed in connection with the Services.

If there are any conflicts between this this section and any other provision of this Privacy Policy, the policy or portion that is more protective of Personal Data shall control to the extent of such conflict. If you have any questions about this section or whether any of the following applies to you, please contact us at privacy-rights@ensighten.com. Note that we may also process Personal Data of our customers' end users or employees in connection with our provision of certain services to customers, in which case we are the processor of Personal Data. If we are the processor of your Personal Data (i.e., not the controller), please contact the controller party in the first instance to address your rights with respect to such data.

Personal Data We Collect

The "Categories of Personal Data We Collect" section above details the Personal Data that we collect from you.

Personal Data Use and Processing Grounds

The "How We Use Your Personal Data" section above explains how we use your Personal Data.

We will only process your Personal Data if we have a lawful basis for doing so. Lawful bases for processing include consent, contractual necessity and our "legitimate interests" or the legitimate interest of others, as further described below.

- **Legitimate Interest:** We process the following categories of Personal Data when we believe it furthers the legitimate interest of us or third parties:
 - Personal identifiers, device/IP data, web analytics, other identifying information that you voluntarily choose to provide, professional or employment-related data, geolocation data.
 - We may also de-identify or anonymize Personal Data to further our legitimate interests.
 - Examples of these legitimate interests include:
 - Providing, customizing and improving the Services.
 - Marketing the Services.
 - Corresponding with you.
 - Meeting legal requirements and enforcing legal terms.
 - Completing corporate transactions.
- **Contractual Necessity:** We process the following categories of Personal Data as a matter of “contractual necessity”, meaning that we need to process the data to perform under our Terms of Use with you, which enables us to provide you with the Services. When we process data due to contractual necessity, failure to provide such Personal Data will result in your inability to use some or all portions of the Services that require such data.
 - Personal identifiers, other identifying information that you voluntarily choose to provide, professional or employment-related data.
- **Consent:** In some cases, we process Personal Data based on the consent you expressly grant to us at the time we collect such data. When we process Personal Data based on your consent, it will be expressly indicated to you at the point and time of collection.
- **Other Processing Grounds:** From time to time we may also need to process Personal Data to comply with a legal obligation, if it is necessary to protect the vital interests of you or other data subjects, or if it is necessary for a task carried out in the public interest.

Sharing Personal Data

The “How We Share Your Personal Data” section above details how we share your Personal Data with third parties.

EU Data Subject Rights

You have certain rights with respect to your Personal Data, including those set forth below. For more information about these rights, or to submit a request, please email us at privacy-rights@ensighten.com. Please note that in some circumstances, we may not be able to fully comply with your request, such as if it is frivolous or extremely impractical, if it jeopardizes the rights of others, or if it is not required by law, but in those circumstances, we will still respond to notify you of such a decision. In some cases, we may also need to you to provide us with additional information, which may include Personal Data, if necessary, to verify your identity and the nature of your request.

- **Access:** You can request more information about the Personal Data we hold about you and request a copy of such Personal Data.
- **Rectification:** If you believe that any Personal Data we are holding about you is incorrect or incomplete, you can request that we correct or supplement such data.
- **Erasure:** You can request that we erase some or all of your Personal Data from our systems.

- **Withdrawal of Consent:** If we are processing your Personal Data based on your consent (as indicated at the time of collection of such data), you have the right to withdraw your consent at any time. Please note, however, that if you exercise this right, you may have to then provide express consent on a case-by-case basis for the use or disclosure of certain of your Personal Data, if such use or disclosure is necessary to enable you to utilize some or all of our Services.
- **Portability:** You can ask for a copy of your Personal Data in a machine-readable format. You can also request that we transmit the data to another controller where technically feasible.
- **Objection:** You can contact us to let us know that you object to the further use or disclosure of your Personal Data for certain purposes, such as for direct marketing purposes.
- **Restriction of Processing:** You can ask us to restrict further processing of your Personal Data.
- **Right to File Complaint:** You have the right to lodge a complaint about Enighten's practices with respect to your Personal Data with the supervisory authority of your country or EU Member State. A list of Supervisory Authorities is available here: https://edpb.europa.eu/about-edpb/board/members_en.

Transfers of Personal Data

PRIVACY SHIELD FRAMEWORK NOTICE

Privacy Shield Principles.

Enighten participates in the Privacy Shield Framework, a set of Principles promulgated by the U.S. Department of Commerce in consultation with the European Commission to protect personal data transferred to the United States. A list of participants in Privacy Shield can be found at <https://www.privacyshield.gov/list>. Enighten is committed to adhering to the Privacy Shield Principles, stated at <https://www.privacyshield.gov/article?id=OVERVIEW> (the "Principles"), with respect to all Personal Data received from the European Union in reliance upon the Privacy Shield. The Principles include, among other things, respect for the choices of data subjects concerning the disclosure of their personal data, maintenance of appropriate security measures to safeguard such data, and commitment to comply with obligatory dispute resolution mechanisms.

Tagman, Ltd., a wholly-owned subsidiary of Enighten based in the United Kingdom, also adheres to the Privacy Shield Principles.

Data Protection Rights.

You have the right to access, review, modify, and delete any personal information which has previously been provided about you that Enighten holds, or which has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to your privacy in the case in question, or where the rights of other persons would be violated.

To contact Enighten with any inquiries or complaints regarding the collection or use of personal data, email privacy-rights@ensighten.com, or address correspondence to Enighten, Inc., Attention: Privacy & Security Department, 887 Oak Grove Avenue, Suite 203, Menlo Park, CA 94025. In the United Kingdom

Ensignten can be contacted via Tagman Ltd., Attention: Privacy & Security Department, Henry Wood House, 2 Riding House Street, London W1W 7FA.

For security purposes, Ensignten only fulfills requests for the personal data associated with the particular email address used to transmit the request. Ensignten may need to verify the identity of the person submitting the request.

Each Ensignten customer sets its own policies concerning whether and what personal information it collects, stores or uses through the use of Ensignten services. All questions about how an Ensignten customer collects, stores or uses personal data, and requests to review, modify, and delete personal data that was collected by an Ensignten customer, should be addressed directly to that customer.

Legally Required Disclosure.

Ensignten may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Ensignten's accountability for personal data that it receives in the United States under the Privacy Shield Framework and subsequently transfers to a third party is described in the Principles. In particular, Ensignten remains responsible and liable under the Principles if third-party agents that it engages to process personal data on its behalf do so in a manner inconsistent with the Principles, unless Ensignten proves that it is not responsible for the event giving rise to the damage.

Disputes and Recourse.

Ensignten is committed to cooperate with the European data protection authorities ("DPAs"), listed at http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm, to provide recourse for individuals to whom the data relate; follow up procedures for verifying that the attestations and assertions Ensignten has made about its privacy practices are true; and remedies for problems arising out of its failure to comply with the Principles. Ensignten will (i) cooperate with the DPAs in the investigation and resolution of complaints brought under the Privacy Shield; (ii) comply with any advice given by the DPAs, where the DPAs take the view that Ensignten needs to take specific action to comply with the Privacy Shield Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles; and (iii) provide the DPAs with written confirmation that such action has been taken.

Ensignten also will comply with the authority of the Swiss Data Protection and Information Commissioner (see <https://www.edoeb.admin.ch/edoeb/en/home.html>), who can be contacted at info@edoeb.admin.ch.

Individuals to whom the data relate also may invoke binding arbitration before the Privacy Shield Panel, to resolve claims not resolved through the above mechanisms, that Ensignten has violated the Privacy Shield Principles. A list of authorized arbitrators, chosen on the basis of independence, integrity, and expertise, is developed by the U.S. Department of Commerce and the European Commission.

Ensignten is also subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

PART V. OTHER IMPORTANT INFORMATION

Other websites

Please be aware that we are not responsible for the privacy practices of other websites that are linked to from our Websites. We encourage our visitors to be aware when they leave our Websites and to read the privacy statements or policies of each and every website that they visit.

Changes to Our Privacy Policy

If we change our Privacy Policy, we will post those changes on this page in addition to updating the “Last Updated” date at the top of this webpage. If we make material changes, we will notify you more directly, for example by posting a notification or message on the Websites and/or in our Services or by emailing you prior to such changes taking effect. We encourage you to review this Privacy Policy frequently to stay informed of the latest modifications.

How to Contact Us

If you have any questions related to this Privacy Policy, our collection of your personal information or to submit request for access or erasure of your data, please contact privacy-rights@ensighten.com. For your protection, we only fulfill requests for the Personal Data associated with the particular email address that you use to send us your request, and we may need to verify your identity before fulfilling your request. If you feel that your complaint has been addressed incompletely, we invite you to let us know for further investigation.

Should you have other questions or concerns about this Privacy Policy, the practices of this site or Ensignten Services, then you may also contact us using the below information:

Ensignten, Inc.
Attn: Privacy & Security Department
887 Oak Grove Avenue, Suite 203
Menlo Park, CA 94025