Sift Service Privacy Notice | Updated July 24, 2025

Our Commitment to Privacy

Sift Science, Inc. (**"Sift"**, **"we"** or **"us"**) respects your privacy and wants you to be informed about what we do. Sift provides a suite of digital trust and safety products and services (the **"Sift Services"**) designed to help online businesses (our **"Customers"**) detect and prevent fraud, security threats, and other illegal or malicious behavior on their digital properties, such as their websites and mobile applications (**"Customer Sites"**).

This Service Privacy Notice (this **"Notice"**) explains who we are and how we collect, share, and use personal information about you when: (i) you use the Sift Services as an authorized end user under our Customer's (your employer's) account (**"Authorized User"**); or (ii) you interact with any of the Customer Sites that use the Sift Services as a digital end user or we otherwise process your information on behalf of our Customers for fraud detection and prevention and/or other related purposes (**"End User"**). We also include information about how you can exercise your privacy rights. **"You"** or **"your"** may be an End User and/or Authorized User depending on the context.

Please note that this Notice does not describe our collection and use of personal information when visitors access our website. For information about how we collect and use information via our website (www.sift.com and its subdomains), please see our Website Privacy Notice.

Additionally, if you are an Authorized User and a resident of California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah or Virginia, please also review our Supplemental U.S. State Law Privacy Notice.

Quick links

We recommend that you read this Notice in full to ensure that you are fully informed. However, if you would like to access a particular section of this Notice, then you can click on the relevant link in the Table of Contents to jump directly to that section.

PART I. GENERAL INFORMATION AND KEY TERMS

Who we are

Sift is a Software-as-a-Service (SaaS) company based in San Francisco, California. We help our Customers detect and address fraud and other illegal or malicious behavior on their

Customer Sites and in other contexts using our proprietary real-time machine learning technology.

In doing so, we need to collect and process information about our Customers' End Users. Our cloud-based machine learning platform uses this information to predict and prevent fraudulent and other illegal or malicious activity in real time.

We offer four core products and related support and knowledge sharing services: Payment Protection (reduces fraudulent payments), Account Defense (reduces fake account creation and prevents bad actors from accessing trust-worthy accounts), Content Integrity (protects Customer Sites from malicious content) and Dispute Management (helps Customers manage chargebacks). You can find out more about these offerings here.

How the Sift Services work

Customers provide us with data and information about End Users and their interactions with the applicable Customer Sites through our Application Programming Interfaces (APIs), and other integrations. We may receive this information directly from our Customers or from their service providers and partners. In addition, we collect data directly from End Users through standard tracking technologies (like our JavaScript code or SDK), which our Customers can embed on their Customer Sites. We refer to all of this data as **"Customer Data"** - as described in Part II below.

We then process the Customer Data through our cloud-based machine learning platform to return a relative fraud score, which is a numerical indicator of the likelihood of fraud or illegal activity for a particular event on the Customer Site (e.g., a purchase transaction, the posting of content, creation of a profile). This involves extracting and deriving the most useful features of the Customer Data, based on new and existing fraud patterns, and identifying connections among data attributes across our entire Customer network. For our Dispute Management product, we process Customer Data to create a dispute win rate which (similar to the fraud score) is a numerical indicator of the likelihood of winning a particular chargeback. In addition to the fraud scores and win rates, we provide our Customers with supporting evidence, analysis of transactional patterns and behavioral signals, records and aggregated reporting and insights across the entire network to highlight potential illegal acts or security threats. These insights may include synthesized summaries and risk assessments based on a combination of structured data analysis and automated content generation technologies.

The data we provide to Customers, including fraud scores, dispute win rates, supporting evidence, transactional and behavioral analysis, and aggregated insights across our network, are used by Customers to assist them in identifying and preventing fraudulent activity on their Customer Sites and managing chargeback disputes. This information may also be used by certain Customers to support their legal or regulatory reporting obligations and risk management procedures (e.g., in relation to their anti-money laundering (AML) or know your customer (KYC) requirements). It is up to Customers to decide what action to take or not to take using the information we provide. For example, depending on the rules set by our Customers,

transactions or activities with certain scores may be required to complete further authentication, flagged for the Customer's review, or blocked. Typically, however, the transaction or activity will proceed with no issues. Customers also provide us with ongoing feedback on the accuracy of the scores by reviewing the activity on their Customer Sites, which in turn improves our proprietary modeling and algorithms. For more information on how our fraud services work, please email privacy@sift.com.

We also may provide security notification and verification features (including two-factor authentication) as part of our Account Defense product. To provide these features, we use certain Customer Data provided by our Customers to send notifications to End Users (such as via text, messages or emails), including to notify End Users of login attempts and account activity, or to send verification codes to End Users, which they enter on the Customer Sites to confirm their identity when logging in or creating new account.

PART II. WHAT WE COLLECT AND HOW WE USE IT

(A) END USERS

Information We Collect About End Users

Information provided by our Customers: Our Customers decide the type of Customer Data they wish to send to Sift for analysis within the Sift Services. Our solutions and support teams work closely with Customers to assess the utility of the specific Customer Data they send to us. For example, Sift guides Customers as to whether a particular data type (e.g., billing method) may be relevant in assessing the particular activity (e.g., likelihood of stolen payment credentials). While it will depend on the specific product offering and Customer relationship, the Customer Data that Customers typically send to us through our integrations include:

- **Contact details** (such as your email address, postal address, phone number, and user login);
- **Information about your device** (such as your IP address, session ID, mobile/desktop device properties, and metadata);
- **Account activity information** (such as account login attempts and failures, when you've reset your password, and other information about your behavior on a Customer Site);
- **Transaction information** (such as information about items you've purchased, currency codes, billing method, invoice details, and partial credit card information);
- **Customer Site communication information** (such as feedback, messaging, Customer support communications, reviews or images you may have provided on or within Customer Sites);
- **KYC-related information** (such as information about whether a KYC check was initiated by the Customer and the result of the check); and

- **Dispute-related information** (such as dispute case number, dispute ID, dispute stage and status, merchant ID, and whether a chargeback was issued or an order was cancelled)

Information we automatically collect when you visit Customer Sites: As further explained below, we use certain standard tracking technologies to automatically collect certain information about your device when you interact with and use Customer Sites. Some of this information (including, for example, your IP address and certain unique identifiers), may identify a particular computer or device and may be considered “personal information” or "personal data" in some jurisdictions, including the EU. Depending on whether you visit a Customer Site via an app or a webpage, the information we collect includes:

- **Browser and device information,** such as the device type and model, architecture, including manufacturer, operating system type and version (e.g. iOS or Android), audio, web browser type and version (e.g., Chrome or Safari), user-agent, carrier name/code and country code, time zone, the network connection type, IP address, hardware-based identifiers (e.g., MAC address) and concurrency, host name, device identifiers (such as iOS Identifier for Vendor (IFV), Android/Google Advertising ID (AAID or GAID)), canvas fingerprint, characteristics related to emulation or rooted (such as if your device is "jailbroken"), and app name and version. We also collect video card hash, cpu class, device memory, indexed db, character set, host name, language, page title and URL, referrer URL, number of fonts, fonts, fonts preference, fonts hash, colors (including inverted and forced), color gamut, monochrome, contrast, color depth, number of plugins, plugins hash, screen height and width, screen frame and resolution, platform, math fingerprint, audio fingerprint, cookie footprint, vendor and vendor flavors, reduced motion, hdr, maximum touchpoints, touch support, open database, JavaEnabled, session storage, local storage, whether the resolution has been tampered, languages or OS, whether ad or DOM blocking is enabled, cookies are enabled, PDF viewer is enabled, whether global privacy control or do not track is enabled, high dynamic range, flash socket IP and flash identifier. The SDK will also collect phone-related metadata (battery level, device properties, carrier name); and
- **Information about an End User’s behavior on Customer's Sites,** such as information about the activities on those Customer Sites, session ID, session start/stop time, timezone offset, and location information which may be general location information inferred from your IP address or, in some circumstances, more precise geolocation information based on latitude and longitude coordinates. You may be able to control the collection of location information through particular Customer Sites by changing the preferences on your mobile device.

Information we collect from third party sources: We may receive some of the information above from our Customer's service providers or partners (such as, their payment processors, customer support providers or KYC providers), as directed by our Customer. We also combine or enhance the information we collect about you with limited information we receive from third parties. For example, we receive information such as whether an IP address is commercial or private, whether a phone number is a landline, whether an email domain is free, or the issuing

bank associated with a transaction. We also work with a small number of providers that match information from social media with End Users' email addresses provided to us, or provide us with a human-readable, mapped location based on a physical address or latitude/longitude.

How We Use End User Information and the Legal Bases

Sift uses information about End Users to provide, maintain, improve, and develop the Sift Services and to comply with our legal obligations.

For example, we process personal information through our cloud-based machine learning platform to return fraud scores to our Customers for particular events or activities on the Customer Site and to return win rates for particular chargeback disputes. Additionally, we process personal information to identify connections among data attributes across our Customer network and to generate transactional and behavioral analysis, along with aggregated reporting and insights. We also process personal information to optimize and improve the Sift Services (for example, to train our proprietary models and algorithms so that we can more effectively detect fraudulent behaviors and ensure the accuracy and integrity of our models and algorithms). In addition, when our Customers use the Sift security notification and two-factor authentication features, we process personal information, such as their End Users' telephone number or email address, to notify End Users of login attempts and account activity and send a verification code to End Users via text message or email. This allows our Customers who use these features to identify suspicious logins and validate their End Users' identities when they log into the Customer Sites or create a new account. Finally, we may also process personal information to validate the identity of End Users seeking to exercise their privacy rights.

We base our processing of your personal information on: (i) our legitimate interests in operating the Sift Services, including to better detecting and preventing fraud, security threats, and other illegal or malicious behavior on Customer Sites; and (ii) our (and our Customers) legitimate interest in combating fraud, maintaining safe online experiences for our Customers and their End Users and reducing the costs associated with invalid or fraudulent chargebacks. In some cases, we may also need to process your personal data to comply with our legal obligations.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, including any legitimate interests relied upon, please contact us as provided under the How to Contact Us section at the end of this Notice.

How We Use Tracking Technologies to Collect Information about End Users

We use standard tracking technologies to automatically collect certain information (as described in the Information We Collect About End Users section) from your device and/or browser when you visit or interact with Customer Sites.

We use the following tracking technologies:

- **JS Snippet:** A JavaScript code (**"JS Snippet"**), also called a tag or pixel, is a tiny snippet of code inserted into the content of the Customer Site. You can disable JavaScript by changing the settings on your browser. Information about the procedure to follow to change the settings can usually be found on your internet browser provider's website via your help screen. Because Sift does not control these settings, we encourage you to check the information provided about them on a regular basis to ensure you are aware of any relevant changes.
- **Mobile "SDKs" or "Software Development Kits":** These are blocks of code that are embedded into a Customer Site that allow Sift to collect certain information as further described above. You can control the use of certain information Sift collects through the SDK by following the instructions applicable to your mobile device operating system, which are usually available in your mobile device settings. This typically means that you will no longer be associated with your old device ID or the information collected about you when the old device ID was assigned to you. However, if the Customer Site you visit requires you to login (e.g., via an email address), Sift will associate a new device ID with your login and your new and old device IDs will be associated. You may also be able to control the collection of location information by particular Customer Sites by changing the preferences on your mobile device. Because Sift does not control these settings, we encourage you to check the information provided about them on a regular basis to ensure you are aware of any relevant changes.
- **Canvas Fingerprinting:** We use canvas fingerprinting, which is a tracking technique that allows us to render graphic images from built-in features of HTML5 Canvas in your browser. The canvas image is often rendered differently on different devices because of a number of factors (such as, your web browser version, operating system and its settings, and installed graphics hardware), and this will allow us to distinguish you from other End Users. If you would like to disable canvas fingerprinting, you may choose to disable JavaScript or download a browser extension that blocks canvas fingerprinting techniques; however doing so may impair the functionality of the Sift Services. Because Sift does not control these settings or extensions, we encourage you to check the information provided about them on a regular basis to ensure you are aware of any relevant changes.

When an End User views or uses a Customer Site, Sift servers are notified, and we are able to collect information from the browser or application as described above.

Automated Decision-Making and Profiling

Sift employs profiling techniques to detect and prevent fraud, security threats and other illegal or malicious behavior on Customer Sites. This includes collecting and analyzing information about End User interactions and behavior across our entire Customer network, and establishing connections between these interactions by linking common data attributes. This also includes using Customer Data to train Sift's global models that understand fraud patterns across our network of Customers, and custom models that are tailored to specific Customer businesses. As a result, profiling not only assists with immediate fraud prevention but plays a crucial role in the

development and improvement of Sift's fraud detection systems, including to ensure the ongoing accuracy and integrity of our models and algorithms.

Automated decision-making refers to decisions that are made automatically on the basis of computer determinations (using software algorithms), without human review or intervention, and that result in legal or significant effects. While the services we provide to our Customers do not generally involve automated decision-making, there are limited circumstances where a Customer's use of the Sift Services may result in such decisions being made about an action you have taken on a Customer Site. For example, a Customer may use the analysis we provide them to automatically pause the completion of an activity or transaction based on rules the Customer has set or to automatically challenge a particular chargeback. In such instances, you may be required to take further steps (e.g., two-factor authentication), you may potentially be unable to complete a transaction, or your chargeback may be disputed by the Customer.

Our Customers decide how to use the scores and insights that we provide them. They set and control the thresholds for any automated actions, which may depend on factors like the Customer's industry, business objectives and risk tolerance. By providing information to Customers, our aim is to empower them to make informed decisions. If you want to learn more about how a business you interact with uses Sift, or you want to contest a decision that's been made by a business that uses Sift, we encourage you to reach out to that online business to assist you.

(B) AUTHORIZED USERS

Information We Collect About Authorized Users

Information you provide to us when you use the Sift Services: You (or your organization's administrator) may provide certain personal information to us through the Sift Services – for example, when you register for the Sift Services, when you consult with our customer support or participate in our online community, send us an email or communicate with us in any way in connection with the Sift Services.

The personal information we collect may include:

- **Business contact information**(such as your name, job title, organization, address, and email address);
- **Account log-in credentials** (such as your username and password);
- **Troubleshooting and support data** (which is data you provide when you contact Sift for help, such as the products you use, and other details that help us provide support); and
- **Payment information** (if you pay for the Sift Services, our payment processor will collect certain information required to process your payment, such as your credit card number and associated identifiers, billing address and background information. Sift does not store full credit card data).

If you ever communicate directly with us or within our community, we may maintain a record of those communications and responses.

Information we collect automatically when you use the Sift Services: In connection with your organization's deployment and use of the Sift Services, we may automatically collect certain device and usage data about Authorized Users when they interact with and use the Sift Services (we call this information "Usage Data"). We (or our third party service providers) use cookies, web beacons, and other tracking technologies to collect some of this information. Please review the Sift Website Cookie Notice for further information.

Usage Data may include:

- **Usage data** (such as the dates and times you access the Sift Services, page views, which activities and features you use, the links you click on, and how you interact with the Sift Services);
- **Device data** (such as IP address, device type, operating system and Internet browser type, screen resolution, operating system name and version, device manufacturer, and model);
- **Device event information** (such as system activity, error reports (sometimes called 'crash dumps'), and hardware settings); and
- **Log files** automatically generated during the use of the Sift Services (such as access times, hardware, and software information).

How We Use Authorized User Information and the Legal Bases

We collect and process personal information for the purposes and on the legal bases identified below. For these purposes, we combine data we collect from different contexts (for example, from your use of two products within the Sift Services). We use this information to:

- **Provide the Sift Services:** We base our processing of your personal information on our legitimate interests to operate and administer the Sift Services. For example, to process transactions with you, authenticate you when you log in, provide customer support, allow you to share knowledge about the Sift Services with us and our support community, and operate and maintain the Sift Services;
- **Promote the security of the Sift Services:** We process your personal information by tracking use of the Sift Services, creating aggregated, non-personal information, verifying accounts and activity, monitoring suspicious or fraudulent activity, and enforcing our terms and policies, to the extent this is necessary for our legitimate interest in promoting the safety and security of the Sift Services, systems, and applications and in protecting our rights and the rights of others;
- **To improve and develop the Sift Services:** We use your personal information (including Usage Data as described in the Information We Collect About Authorized Users section) to identify trends, usage, activity patterns, and areas for integration and improvement of the Sift Services so that we continually improve the Sift Services, including adding new features or capabilities that make the Sift Services smarter, faster,

secure, integrated, and more useful to our Customers and their Authorized Users to the extent it is necessary for our legitimate interests in developing and improving the Sift Services, or where we seek your consent;

- **To communicate with you about the Sift Services:** We may send you service, technical, and other administrative or transactional emails, messages, and other types of notifications to in reliance on our legitimate interests in administering the Sift Services. These communications are considered part of the Sift Services and in most cases you cannot opt-out of them. If an opt-out is available, you will find that option within the communication itself or in your account settings;
- **Send you marketing communications:** We will process your personal information to send you marketing information, product recommendations, events, promotions, contests, and other non-transactional communications (e.g., emails, telemarketing calls, SMS or push notifications) about us in accordance with your marketing preferences as necessary for our legitimate interests in conducting direct marketing or to the extent you have provided your prior consent (please see the Unsubscribe From Our Mailing List section below);
- **To protect our legitimate business interests and legal rights:** Where required by law or where we believe it is necessary to protect our legal rights, interests, and the interests of others, we use information about you in connection with legal claims, compliance, regulatory, and audit functions, and disclosures in connection with the acquisition, merger, or sale of a business; and
- **With your consent:** We use information about you where you have given us consent to do so for a specific purpose not listed above. For example, we may publish testimonials or featured customer stories to promote the Sift Services with your permission.

(C) SHARING INFORMATION WITH THIRD PARTIES

We may share and disclose information about End Users and Authorized Users in the following circumstances:

- **Vendors, consultants and other service providers**
  We may share your information with third party vendors, contractors, consultants, and other service providers who provide data processing services to us and with whom the sharing of such information is necessary to undertake that work. If you are an Authorized User, examples of the type of service providers include: processing billing, providing customer support, identity verification, or hosting our infrastructure. We may use providers who assist us in delivering online and offline marketing optimizations. If you are an End User, examples of these types of service providers include: hosting our infrastructure, security notification and verification services (including two-factor authentication services), assisting with implementation, manual review and labeling, and supporting data interpretation and content synthesis, and for data enrichment purposes (described below).
- **Our Customers and their vendors, service providers and other intermediaries**
  We may share your information with our Customers, as well as our Customers' vendors,

service providers, and other third parties acting under their direction, where such sharing is necessary to provide the Sift Services and fulfill the Customer's request. For example, if you are an End User we may share your information with our Customers' payment processors or the issuing or acquiring bank involved in a chargeback.

- **Third-party vendor integrations**
  We may offer Customers the ability to use third party vendor integrations through our Services. If you choose to use these third party vendor integrations, then you are directly interacting with that third party vendor and providing or directing us to provide information, including personal information, to them for purposes of facilitating the integration.
- **Data enrichment providers**
  We may share certain Customer Data (e.g., email addresses) with select third-party service providers (e.g., location data providers or identity verification providers) for data enrichment purposes. Enriching data allows us to make more informed fraud risk assessments. For example, we may work with providers that match information from social media with End Users' email addresses provided to us, that provide us with a human-readable, mapped location based on a physical address or latitude/longitude. Sift requires that any information disclosed to a provider is used only to perform their service and not for any incompatible purpose, and only as allowed by applicable law.
- **Professional advisors**
  We may disclose your personal information to professional advisors, such as lawyers, bankers, auditors and insurers, where necessary in the course of the professional services they render to us.
- **Compliance with laws**
  We may disclose your information to any competent law enforcement body, regulator, government agency, court or other third party where we believe disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend our legal rights, or (iii) to protect your vital interests or those of any other person (see below).
- **Vital interests and legal rights**
  We may disclose information about you if we believe it necessary to protect the vital interests or legal rights of Sift, you or any other person.
- **Corporate affiliates and transactions**
  We may provide your information to our affiliates (meaning any subsidiary, parent company or company under common control with Sift). Our affiliates will use your information only for the purposes described in this Notice. Additionally, if Sift is involved in a merger, acquisition or sale of all or a portion of its assets, your information may be shared or transferred as part of that transaction, as permitted by law.

PART III. INTERNATIONAL TRANSFERS

Processing of personal information in the US and other territories

Your personal information may be transferred to, and processed by Sift in, countries other than the country in which you are resident, including the United States, Ukraine and other countries around the world where Sift, its affiliates, service providers or partners operate facilities. These countries may have data protection laws that are different to the laws of your country and may not provide for the same level of protection as your jurisdiction. However, regardless of where your data is processed, we take steps to ensure that your personal information will be processed in accordance with this Notice and the requirements of applicable law.

European data transfers

If you are located in the European Economic Area ("**EEA**"), United Kingdom ("**UK**"), or Switzerland, we will protect your personal information when it is transferred outside of your jurisdiction by: (i) processing it in a territory that provides an adequate level of protection for personal information based on the receiving country's data protection laws; and/or (ii) implementing appropriate safeguards to protect your personal information, such as requiring the recipient to comply with the Standard Contractual Clauses, or another lawful and approved transfer mechanism.

PART IV. YOUR PRIVACY RIGHTS

Depending on your location and subject to applicable law, you may have the following rights with regard to personal information we control about you:

Access, review, correct, or delete your information

Depending on your location, you may have the right to access, request correction or deletion of any personal information that we process about you, as provided under applicable data protection laws. You can send an email to privacy@sift.com or use our web form to exercise these rights.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws, and treat each according to the requirements of the applicable jurisdiction. To protect your privacy and security, we may need to take reasonable steps to verify your identity before responding to your request. Specifically, we (or our third party service provider acting on our behalf) may need to collect a copy of your photo ID and any other information necessary to confirm your identity. Such information will be securely processed in accordance with this Notice and only used for the purpose of verifying your identity.

Please note that, in certain circumstances, your ability to access or control your personal information may be limited, as required or permitted by applicable laws. For example, Sift may be required by law to retain and continue processing your personal information after a deletion request, for example where such processing is necessary to maintain the accuracy and integrity

of our models and algorithms so that we can more effectively detect fraudulent behaviors or assist with chargeback disputes within the permissible timeframe.

European Privacy Rights: EEA, UK and Switzerland

If you are located in the EEA, UK, or Switzerland, you have certain rights under applicable data protection laws, including the General Data Protection Regulation ("**GDPR**").

Access, correction and deletion: You have the right to obtain information about the processing of your personal information, including automated decision-making and profiling, and to receive a copy of your personal information. You may also request correction or deletion of any personal information that we process about you. You can send an email to privacy@sift.com or use our web form to exercise these rights. As explained above, in certain circumstances, exceptions may apply to these rights as required or permitted under applicable laws. For example, Sift may retain your personal information after a deletion request to ensure the accuracy and integrity of our models and algorithms or to assist with chargeback disputes within the permissible timeframe.

Objection to processing, rectification and portability: You have the right to object to the processing of your personal information, ask us to restrict the processing of your personal information, request manual review of automated decisions, or request portability of your personal information. To exercise these rights, please email privacy@sift.com or submit a request via our web form. Again, exceptions may apply to these rights as required or permitted under applicable laws. For example, Sift may continue to process your personal information after an objection request to ensure the accuracy and integrity of our models and algorithms.

Withdrawal of consent: If we have collected and process your personal information with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent. To withdraw your consent to any processing, please email privacy@sift.com or submit a request via our web form.

Right to complain to a data protection authority: You have the right to complain to a data protection authority about our collection and use of your personal information. For more information, please contact your local data protection authority. Contact details for data protection authorities in the EEA and UK are available here and Switzerland are here.

U.S. State Law Rights

Certain U.S. states have passed laws extending certain privacy rights to their residents, including California, Colorado, Virginia, Utah and other states.

If you are an Authorized User and a resident of California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire,

New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah or Virginia, please review our Supplemental U.S. State Law Privacy Notice, which describes certain disclosures and rights available to you under your state's privacy laws, when such laws are effective.

When we handle personal information in providing the Sift Services to our Customers, we do so as a "service provider" under the CCPA or "processor" under the other state privacy laws set forth above on behalf of our Customers (who are "businesses" under the CCPA and "controllers" under the other state privacy laws), to assist them in protecting against security threats or detecting illegal, criminal, malicious or fraudulent activity. When requested, we reasonably assist our Customers in responding to consumer requests under these U.S. state privacy laws. If you are an End-User, please direct any requests regarding your U.S. state privacy law rights to the businesses you believe may have collected (or transferred to Sift) your information, so that those businesses or controllers can properly instruct us in whether and in how to assist them in responding.

Unsubscribe from our mailing list

You may at any time ask us to stop sending marketing communications to you, including by clicking "Unsubscribe" in any e-mail communications we send you. If you have any questions in relation to the "Unsubscribe" process, please feel free to get in touch via the contact details set out below. If you choose to no longer receive marketing information, we may still communicate with you regarding such things as your security updates, product functionality, responses to service requests, or other transactional, non-marketing/administrative related purposes.

PART V. OTHER IMPORTANT INFORMATION

Security safeguards

We use technical and organizational security measures designed to protect personal information processed as part of the Sift Services against unauthorized access, disclosure, alteration, and destruction.

Data Retention

We retain your personal information where we have an ongoing legitimate business need to do so and for a period of time consistent with the original purpose as described in this Notice. We determine the appropriate retention period for personal information on the basis of the amount, nature and sensitivity of your personal information processed, the potential risk of harm from unauthorized use or disclosure of your personal information and whether we can achieve the purposes of the processing through other means, as well as on the basis of applicable legal requirements (such as applicable statutes of limitation).

After expiration of the applicable retention periods, we will either delete or anonymize your personal information or, 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.

Changes to this Notice

We may revise this Notice from time to time in response to changing legal, technical or business developments, and the revised version will be effective when it is posted. If we make any material changes to the ways in which we use or share personal information previously collected from you, we will prominently post the updated version here and in our discretion notify you and/or the Customer by email or by other reasonable means. You can see when this Notice was last updated by checking the “last updated” or “effective” date displayed at the top of this Notice. You can access previous versions of this notice in our Policy & Terms Archive.

PART VI. HOW TO CONTACT US

Contact Details

Please contact Sift with any questions or comments about this Notice or our privacy practices at:
Sift Science, Inc.
c/o Industrious
Attn: Privacy Office
77 Geary Street, Suite 509
San Francisco, CA 94108
Email: privacy@sift.com

Email: privacy@sift.com

Controller Information, Data Protection Officer and EU and UK Representatives

If you are a resident in the EEA, UK, or Switzerland, Sift Science, Inc. is the controller of the personal information (i.e., personal data under European data protection laws) collected through the Sift Services.

You may contact our Data Protection Officer by emailing dpo@sift.com or using the mailing address listed in the Contact Details section above.

Our EEA representative is:

Sift Science Ireland Limited
by email: privacy@sift.com
by mail: Sift Science Ireland Limited c/o Sift Science, Inc. 77 Geary Street, Suite 509, San Francisco, California CA 94108

Our UK representative is:

Sift Science UK Limited
by email: privacy@sift.com
by mail: Sift Science UK Limited c/o Sift Science, Inc. 77 Geary Street, Suite 509, San Francisco, California CA 94108

Further Privacy Resources

Website Privacy Notice
Supplemental U.S. State Law Privacy Notice
Website Cookie Notice
Data Rights Request
Do Not Sell My Personal Information

Sift Policy & Terms Archive