

NetWitness Privacy Policy

Introduction

Your privacy is important to NetWitness, a business unit of RSA Security LLC so we have developed this Privacy Policy that outlines our privacy practice on how we process, collect, use, and share your personal data as well as your privacy rights under certain privacy laws. We may provide additional data privacy information by using a supplementary privacy notice(s).

In this Privacy Policy, “NetWitness,” “our,” “us,” or “we” refers to NetWitness, a business unit of RSA Security LLC and its relevant affiliate(s) involved in the collection, use, sharing or processing of your personal data.

NetWitness is committed to protecting the privacy and security of all personal data we collect when you access, use, or interact with us via our websites and marketing communications and all personal data we process in order to provide services to our customers. We receive limited personal data from our customers.

This Privacy Policy is intended to apply to the extent NetWitness processes your personal data as a data controller. It is not intended to apply when NetWitness processes your personal data as a data processor on behalf of our customers. It also does not apply to information that has been aggregated, de-identified, or pseudonymized.

1. Information We Collect

We collect “personal data,” which means information relating to an individual who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number, location data, or an online identifier.

1.1 Information Collected from You

The types of information we collect about you depends on your use of our products, services, and the ways that you interact with us, and includes information we obtain from third parties. This may include information about:

- Contact information, such as your name, country, email address, phone number, time zone, mailing address.
- Business information such as your job title, job level, job role/function and other business or company information.
- Interest information such products or services you purchase, and the activities associated with your account and preferences.
- Web form information you provide in our web forms (forms that you choose to complete will indicate whether the information requested is mandatory or voluntary).

- Cookie and tracking information while you interact in our websites include your browser type, IP address, Pixel ID, unique device identification number, operating system, device type, and version information, language settings, webpages you view, the amount of time you spend on pages, the website URL that referred you to our pages, your geographic information derived from your IP address, other technical information and any hyperlinks or advertisements you select.
- Browser referral information about the websites that led you to visit us.
- Error reports and performance information of the products and any problems you experience, including error reports.
- Content consumption information regarding media content (e.g., blog posts, articles, social medial posts) you access .
- Feedback and ratings information you provide to us such as customer survey feedback and product reviews you write, unless anonymous.
- Third party sources' information that may include personal data to supplement the information we have collected about you.
- Third party websites and links. We may provide links to other websites, which if you click on them may collect information about you and direct you to those websites. The information practices of those third-party websites linked to our website are covered by the third party's own privacy policies/statements and we encourage you to read those.
- Credentials such as password hints, and similar security information used for authentication and MyAccount access.
- Demographic information such as your age, gender, country, interests, and preferences.
- Payment information to process payments, such as your payment instrument number (such as a credit card number) and the security code associated with your payment instrument.
- Troubleshooting and help information when you contact NetWitness for technical support or customer support services, phone conversations or chat sessions with our representatives may be monitored and recorded.
- Information necessary for us to provide services to you.
- Any other personal data you choose to share with us.

1.2 Special Categories of Personal Data

We do not intentionally collect special categories of personal data which includes sensitive information such as:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Membership in a trade union
- Genetic data
- Biometric data
- Physical or mental health or condition
- Sex life or sexual orientation

You are not required to provide, nor should you disclose this information as we do not intend to process sensitive information. However, if you do disclose, you acknowledge that you consent to our collecting and processing of these special categories of data.

2. How We Collect Your Personal Data

The types of personal data we collect about you depends upon your use of our products and services and the ways that you interact with us.

2.1 Personal Data Collected Directly from You

We ask for and collect personal data from you in the following instances:

- When you express interest in our products and services and request additional information; when you request a demo; when you request customer support; when you use our Contact Us page; when you register to receive communications from us; when you participate in a program or a survey; when you download content from our websites; when you are an authorized user of our products and services.
 - We may collect your name, job title, company name, address, country, phone number, email address, username, and password.
- When you make a purchase using our websites.
 - We may collect your name, job title, company name, address, country, phone number, email address, and financial information for billing and payment, such as billing name and address, payment instrument such as credit card number and the security code associated with your payment instrument, or bank account information.
- When you register for one of our events.
 - We may collect your name, job title, company name, address, country, phone number, email address, and financial information for billing and payment, such as billing name and address, payment instrument such as credit card number and the security code associated with your payment instrument, or bank account information. If you attend an in-person event and are issued a badge, we may scan the badge and access your information, such as name, job title, company name, address, country, phone number, and email address. We may also collect your image.
- When you communicate with us by phone.
 - We may collect information to verify your identity and may record the call for training purposes, in accordance with applicable laws.
- When you visit our offices.
 - We may collect name, job title, company name, address, country, phone number, email address, and time and date of your arrival. We may also collect your image.
- When you interact with our websites or emails.
 - We may collect information about your device, your usage of our websites and/or emails using cookies, web beacons, or other similar technologies.
- When you interact with our products and services.

- We may collect account history information and the activities associated with your account, such as information about your device and your usage of our products and services through log files and other technologies.
- When you voluntarily fill out a web form, participate in a survey, respond to a questionnaire, or share data with us in another form of research.
 - We may collect information you voluntarily choose to provide and any mandatory information we request.

If you provide personal data relating to another individual, you represent that you have the authority to do so, and where required, you represent that you have obtained the necessary consent to share such data. You acknowledge that the personal data of the other individual may be used in accordance with this Privacy Policy.

If you believe your personal data has improperly been provided to us, or if you want to exercise your rights relating to your personal data, please contact us at privacy@netwitness.com.

2.2 Personal Data Collected from Others

We may collect your personal data from other sources such as publicly available information and third-party sources that we purchase personal data from. The third-party sources may change over time and may include:

- Data brokers from whom we purchase demographic data to supplement the personal data we have collected about you;
- Communication services, including email providers and social networks when you give us permission to access your information from such third-party services or networks;
- Partners with whom we offer co-branded products and services, or with whom we engage in joint marketing activities.

The personal data may include identifiers, professional or employment related information, education information, commercial information, visual information, internet activity information, social media profiles, and inferences about preferences and behaviors. We may combine information from other sources with the personal data provided by you.

This data helps us keep our records updated, identify new customers, and create tailored advertising for products and services that may be of interest to you.

3. Device and Usage Data We Process

We use information gathering tools such as cookies, web beacons, pixels, and similar technology to automatically collect information that might contain your personal data when you use our websites and services or interact with emails we send you.

3.1 Automatic collection

Our websites automatically collect data about you when you visit the websites. This information may include:

- Identifiers
- Commercial information
- IP address
- Proxy Server information
- Device and application information
- Identification numbers
- Location
- Browser type
- Plug-ins
- Integrations
- Internet service provider
- Mobile carrier
- Pages and files viewed
- Searches
- Referring website, app, or advertisement
- System configuration information
- Advertising preferences
- Language preferences
- Date and time stamps of your usage
- Frequency of visits to the websites

We use this information to analyze overall trends, help us improve our websites, offer a personalized experience for website users, and secure and maintain our websites.

We also automatically collect information as part of your use of our products and services. This information may include:

- Identifiers
- Commercial information
- IP address
- Proxy server information
- Mobile device number
- Device identification number
- Application identification number
- Location
- Browser type
- Internet service provider
- Mobile carrier
- Pages and files viewed
- Website and webpage interactions
- Search information

- Operating system type and version
- System configuration information
- Data and time stamps of your usage
- Details of products and product versions you use

We use this information to maintain the security of our websites and our products and services, provide necessary functionality, improve the performance of services, assess and improve customer and user experience, validate that you are an authorized user, review compliance with usage terms, identify future opportunities for service development, assess capacity needs and requirements, and identify customer opportunities.

Device and usage data is primarily used to identify the unique uses of our websites instead of identifying specific individuals unless identity is required for security purposes or to provide services to the individual.

3.2 Tracking Technologies

Our websites, online services, interactive applications, email messages, and advertisements may use tracking technologies such as web beacons, pixels, tags, and cookies to help us tailor your experience, better understand your preferences, tell us which parts of our websites you have visited, and facilitate and measure the effectiveness of our interest-based advertisements and web services, and gather information about the use of our websites and the interactions with our emails.

Web beacons and pixels are used on our websites and in our emails to help deliver cookies, gather usage and performance data, and operate and improve our websites and marketing emails.

Cookies are alphanumeric identifiers that are stored on your device's local storage through your web browser for recordkeeping purposes. Some cookies allow us to make it easier for you to navigate our websites and services, improve and customize your browsing experience, and infer your browsing preferences, while others are used to enable a faster log-in process or allow us to track your online activities over time and across our webpages.

We use both session-based and persistent cookies.

- Session-based cookies only exist during a single session and will disappear from your device when you close your browser or turn off your device. We use session cookies to allow our systems to uniquely identify you during a session or while you are logged into the websites or our services. This allows us to process your online transactions and requests and to verify your identity after you have logged in, as you move through our webpages and services.

- Persistent cookies will remain on your device even after you close your browser or turn off your device. We use persistent cookies to track aggregate and statistical information about user activity on our websites.

There are four categories of cookies:

- **Strictly Necessary:** These cookies allow core website functionalities. The website cannot function properly without these cookies.
- **Functionality:** Functionality cookies are used to remember visitor information on the website, e.g. language, time zone, enhanced content.
- **Advertising:** Advertising cookies track your activity across our websites to understand your interests and to show you personalized marketing.
- **Analytics:** These cookies help improve our website by analyzing and reporting information on how visitors use it.

3.3 Disabling Cookies on Your Browser

Depending on your personal preferences, you can edit your browser options by using the “Help” function in your browser toolbar. You can prevent your computer from accepting new cookies, have the browser notify you when you receive a new cookie, or disable all cookies. However, it is important to note that if you block or delete cookies that we use on our websites, you will still be able to browse certain areas of the websites, but some features may not function properly.

3.4 Flash Local Storage Objects

We may use Flash Local Storage Objects (Flash LSOs) to store your website preferences and to personalize your visit. Flash LSOs are different than browser cookies because of the amount and type of data stored. Typically, you cannot control, delete, or disable acceptance of all Flash LSOs through your web browser. For more information about Flash LSOs and to learn how to manage your settings for Flash LSOs, go to the Adobe Flash Player Help Page.

3.5 Invisible Images

Invisible Images are tiny graphics with a unique identifier, similar in function to cookies. In contrast to cookies, which are stored on your device’s local storage, these images are embedded invisibly on web and application pages.

We may use invisible images, which are also known as web beacons, web bugs, or pixel tags in connection with our websites and service offerings to, among other things, track the activities of website visitors and application users, help us manage content, and compile statistics about website usage.

We, and our third-party service providers, also use invisible images in HTML emails to our customers to help us track email response rates, identify when our emails are viewed, and to track whether our emails are forwarded.

3.6 Behavioral or Interest Based Advertising

We may use information about your visit to our websites, such as pages you visit, items you view, and your responses to our advertisements and emails. This information allows us to make the advertisements you see more relevant to you. To update your preferences, you may click “unsubscribe” in any email marketing communication that is sent to you.

It may take up to ten (10) business days for your email preferences to take effect.

You may also visit the opt out pages to opt out of many third-party advertising networks through various trade association websites such as:

- Internet Advertising Bureau (IAB): Interactive Advertising Bureau (IAB)
- Network Advertising Initiative (NAI): thenai.org
- Digital Advertising Alliance (DAA): DigitalAdvertisingAlliance.org

However, using these opt out pages does not mean that you will no longer receive advertising through our websites or services, or on other third-party websites.

3.7 Cross Device Use

We, and our third-party service providers, including Google, may use the information that we collect about you, whether directly from our website, from our mobile applications, through your device, or from a third party, to help us and our third-party service providers identify other devices that you use, such as a mobile phone, tablet, or other computer.

We, and our third-party service providers may also utilize the cross-device use information we learn about you to serve targeted advertising on your devices and to send you emails.

To opt out of cross device use, you may opt out of third-party advertising (see Section 3.7). However, if you opt out of these advertising cookies, your opt out will be specific to the web browser, application, or device from which you accessed the opt out. If you use multiple devices or web browsers, you will need to opt out of each device and each browser on each device that you use.

3.8 Opt-Out Preference Signals

We do not engage in “sales,” “shares,” or targeted advertising as those terms are defined under applicable laws and therefore, our websites do not recognize the Global Privacy Control (“GPC”) signal. For more information and to download and use a browser supporting the GPC browser signal, click here: <https://globalprivacycontrol.org/orgs>. If

you choose to use the GPC signal, you will need to turn it on for each supported browser or browser extension you use.

Some internet browsers offer a “Do Not Track” option that allows you to tell websites that you do not want your online activities tracked. There is currently no industry common standard, therefore, we do recognize these Do Not Track signals on our websites. We take privacy and your preferences seriously and will continue to monitor Do Not Track developments and the adoption of a standard.

3.9 Social Media

We are responsible for the content we publish using social media platforms, but we are not responsible for managing the social media platforms or the data they collect and process. Our websites have social media sharing plugins. These widgets may allow you to post information about your activities on our websites on outside platforms and social networks. You may also be able to like or share information we have posted on our websites or our branded social media pages. If the social media pages are hosted by the individual platforms and you click through to the site from our websites, the platform may receive information showing that you visited our websites. If you are logged into the social media site at the time you click through, the social media site may be able to link your visit to our websites with your social media profile.

3.10 Telephony Information

If you use features of our services on your mobile device, we may collect telephony log information, including phone numbers, time and date of the calls, duration of the call, SMS routing information. We may collect device event information, such as system activity, hardware settings, and browser language. We may also collect location information through GPS, IP address, WiFi access points and cell towers, and other sensors that provide us with information on nearby devices.

4. Purposes and Legal Bases for Processing Personal Data

We collect and process your personal data for the following purposes:

- To provide and promote our websites, products, and services. We will process your personal data to perform our obligations under any contract we have with you or your employer for the use of our websites and services.
 - If no contract exists, the legal basis for processing your personal data is to operate and administer our websites and services to provide you with access to content.
- To provide and promote the security of our websites. We will process your personal data when we track your use of our websites and services; when we create aggregated, de-identified, pseudonymized data; when we verify accounts and activity; when we investigate suspicious activity; when we enforce our terms and conditions and policies.

- The legal basis for processing your personal data is to promote the safety and security of our websites, services, systems, and applications and to protect our rights and the rights of others.
- To manage users. We will process your personal data when you register for an account with us, to establish and manage the user account, and to allow us to perform our obligations to you in accordance with the applicable contract or terms and conditions.
 - The legal basis for processing your personal data is to allow us to confirm and authenticate your identity and prevent unauthorized access to restricted areas of our websites.
- To provide support. We will process your personal data when you request technical support or customer support services to review error reports, performance information of the products, and the problems you experience, and to troubleshoot and provide help information.
 - The legal basis for processing your personal data is to allow us to confirm the issue and provide the assistance you need to resolve the issue.
- To respond to your requests. We will process your personal data when you fill out a “Contact Us” form, request a demo, or contact us in any other manner, including chatbot, email, or phone.
 - The legal basis for processing your personal data is to perform our obligations to you, fulfill your requests, and communicate with you.
- To manage payments. We will process your personal data when you make a purchase and provide financial information to us.
 - The legal basis for processing your personal data is to collect payments as necessary pursuant to the contracts we have with you.
- To record phone conversations and chat sessions. We will process your personal data if you call us, and we monitor and record the call or if you open a chat session and we monitor and record the conversation.
 - The legal basis for processing your personal data is for training, quality assurance, and administrative purposes. We will obtain your prior consent or allow you to object to a phone call being recorded if required under applicable law.
- To send communications. We will process your personal data to send you marketing information, product recommendations, and other communications, such as newsletters or push notifications.
 - The legal basis for processing your personal data is to provide information about promotions, news, or events for direct marketing purposes.
- To manage event registration. We will process your personal data to plan and host events for which you register or attend, including sending communications to you.
 - The legal basis for processing your personal data is to fulfill our obligations to you.
- To develop and improve our websites and services. We will process your personal data to analyze trends and track your usage of and interactions with our websites, as necessary.

- The legal basis for processing your personal data is for our legitimate interest in developing and improving our websites and services and providing users with more relevant content and service offerings.
- To assess and improve user experience. We will process your device and data usage, which may be associated with your personal data, and content consumption information regarding media content such as blogs, articles, and social media posts you access.
 - The legal basis for processing your personal data is to analyze trends, assess and improve the user experience, and improve our websites and service offerings.
- To assess capacity requirements. We will process your personal data to assess the capacity requirements of our services.
 - The legal basis for processing your personal data is to ensure we have the necessary capacity for our service offerings.
- To review compliance with our terms of use. We will process your personal data to validate that you are an authorized user and to ensure compliance with the terms which grant your use.
 - The legal basis for processing your personal data is to ensure adherence to the relevant terms.
- To identify customer opportunities. We will process your personal data to assess new opportunities for our customers.
 - The legal basis for processing your personal data is to ensure we meet the demands of our customers and their user experience.
- To display personalized advertisements and content. We will process your personal data to advertise to you and provide other personalized content based on your interests and activities.
 - The legal basis for processing your personal data is to tailor your experience with us and make appropriate recommendations.
- To administer surveys and conduct research. We will process your personal data to conduct market research, obtain product reviews, and collect feedback and ratings information as part of a customer survey.
 - The legal basis for processing your personal data is to improve our products and services and meet the goals and purpose of the research.
- To comply with legal obligations. We will process your personal data to cooperate with public and government authorities, courts, or regulatory authorities to meet our legal obligations under applicable laws, to protect our rights, protect against misuse or abuse of our websites or services, protect personal property, protect the safety of others, pursue remedies available to us, limit our damages, comply with judicial proceedings or court orders or legal processes, respond to lawful requests, and to conduct audits.
 - The legal basis for processing your personal data is to comply with applicable laws, rules, and regulations.

Where required by law, we will obtain your prior consent to use and process your personal data, or we will rely on another authorized legal basis, such as performing a contract or having a legitimate interest.

5. Who Do We Share Your Personal Data With?

We may share your personal data with our business partners, which include:

- **Affiliates.** We will share your personal data with our affiliates to the extent it is required on the basis of the affiliate's contract with you.
- **Service Providers.** We will share your personal data with our contracted service providers who provide services such as hosting, email, customer relationship management (CRM), IT and system administration, credit card and payment processing, research and analytics, and customer support.
- **Professional Advisors.** We will share your personal data with our professional advisors, such as lawyers, bankers, auditors, and insurers, to the extent we are legally obligated to share or have a legitimate interest in sharing your personal data.
- **Third Party Networks and Websites.** We will share your personal data with social media networks and advertising websites so we can market and advertise on third party platforms.
- **Third Party Accounts.** We will share your personal data if you connect your third-party accounts through our products in order to authenticate you and fulfill any requests you have through the third-party account.
- **Third Parties in a Corporate Transaction.** We will share your personal data if we are involved in a merger, acquisition, reorganization, dissolution, or other corporate change.

6. International Transfers of Personal Data

We may collect, transfer, and store your personal data in the United States. We may also collect, transfer, and store your personal data in other countries. This includes countries outside the European Economic Area (EEA) and countries with laws that have not been determined to provide an adequate level of protection under the laws of the European Union (EU) or other jurisdictions.

This means that your personal data may be processed outside your jurisdiction in countries that are not subject to an adequacy decision of the European Commission on the basis of Article 45 of Regulation (EU) 2016/679 (GDPR) or regulatory authority. However, we will ensure that your personal data is subject to an adequate level of protection and security by entering into appropriate agreements, including the UK standard contractual clauses and the EU standard contractual clauses, or an alternative mechanism for the transfer of your personal data.

7. Children's Data

Our websites, products, and services are not for children. We do not knowingly collect and process personal data of children under the age of sixteen (16). If you are a parent or guardian and believe your child has provided us with personal data without your consent, please contact us at privacy@netwitness.com and we will take the necessary steps to delete their personal data from our systems.

8. Data Retention

We will retain your information no longer than is necessary for NetWitness' purposes. We will retain your personal data for different periods of time depending on the category of personal data it is collected for. Some personal data may be deleted automatically, and some will be retained longer consistent with the original purpose for collecting it, for as long as required to fulfill our obligations, or as required by law.

When the retention period expires, we will delete your personal data. If there is any data that cannot be completely deleted for technical reasons, we will implement appropriate measures to prevent any further processing of such data.

9. Your Rights

You may have certain rights relating to your personal data, subject to data protection laws. These rights may include:

- Access to your personal data
- Information regarding our processing of your personal data
- Rectification of inaccurate personal data
- Erasure or deletion of your personal data
- Restrictions on our processing of your personal data
- Objection to our processing of your personal data
- Opting out of certain disclosures of your personal data
- No retaliation or discrimination for exercising your rights
- Not being subject to decisions solely based on automated processing
- Withdrawing consent for future processing
- Transferring your personal data to another service provider
- Contacting us with concerns or complaints or make a complaint to your local supervisory authority

We do not currently use automated decision making on our websites or in our services.

9.1 How to Exercise Your Rights

To exercise your rights, please contact us at privacy@netwitness.com.

Your personal data may be processed by us when we respond to these rights. We attempt to respond to all legitimate requests within thirty (30) days, unless otherwise required by law, and will contact you if we need additional information in order to honor your request or verify your identity. At times and as permitted by applicable law, it may take longer than thirty (30) days, considering the number and the complexity of the requests we receive. We will contact you if we need additional time to fulfill your request.

Some authorized users may update their settings and profiles by logging into their accounts.

Please be aware that your request does not guarantee complete access or comprehensive removal as the law may not permit or require removal in certain circumstances.

9.2 Your Rights in Customer Data

We may process your personal data if submitted by or for a customer of our products and services. We are the data processor on behalf of our customer, who is the data controller. We are not responsible for and have no control over the privacy and data security practices of our customers, which may differ from those in our Privacy Policy.

If your data has been submitted to us by or on behalf of a customer and you wish to exercise any rights you have over your personal data under the applicable data protection laws, please inquire directly with our customer.

We may only access your personal data based upon our customer's instructions. If you wish to make your request to exercise your rights with us, please provide us the name of the customer who submitted your data to us. We will refer the request to that customer and provide any support they need to respond to your request within a reasonable time.

9.3 Your Preferences for Email and SMS Communications

You have choices about how we reach you with marketing offers and about other uses of your information. To update your preferences, you can:

- Click "unsubscribe" in any email marketing communications we send you or click [here](#).
- Visit our Preference Management Center to select your choices.

Please be aware that it may take up to 10 business days for your email preferences to take effect.

Opting out of marketing communications will not opt you out of receiving important business communications related to your current relationship with us, such as information about your products or services, event registrations, service announcements, or security information.

10. How we Secure Your Personal Data

We take appropriate organizational, technical, and physical measures to help safeguard against accidental or unlawful destruction, loss, alteration, and unauthorized disclosure of, or access to, the personal data we collect and process. However, no method of collection, storage, or transmission is 100% secure. You are solely responsible for protecting your password, limiting access to your devices, and signing out of websites after your sessions.

11. Linked Sites

For your convenience, there may be hyperlinks on our websites that link to other websites. We are not responsible for, and this Privacy Policy does not apply to the privacy practices of any linked websites or of any companies that we do not own or control. The website links may collect information in addition to the information we collect.

We do not endorse any of these linked websites, their products, services, or any of the content on their websites. We encourage you to seek and read the privacy policy of each linked website that you visit to understand how the information that is collected about you is used and protected.

12. Notice to California Residents

The California Consumer Privacy Act, as amended by the California Privacy Rights Act (CCPA), requires that we provide California residents with a privacy policy that contains a comprehensive description of our online and offline practices regarding the collection, use, disclosure, sale, sharing, and retention of personal information and of the rights of California residents regarding their personal information. This section of the Privacy Policy is intended solely for, and is applicable only as to, California residents. If you are not a California resident, this section does not apply to you and you should not rely on it.

The CCPA defines “personal information” to mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California resident or household. Personal information does not include publicly available, deidentified or aggregated information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this “**Notice to California Residents**” section we will refer to this information as “Personal Information.”

If there is any conflict between this Section 12 and the rest of our Privacy Policy, the terms of Section 12 shall prevail as to the personal data of California residents that is subject to the CCPA.

Notice at Collection of Personal Information

We currently collect and in the preceding twelve (12) months, we have collected the following categories of Personal Information:

- Identifiers (name, postal address, email address, IP address, and other similar identifiers)
- Personal information described in California’s Customer Records statute (California Civil Code § 1798.80(e)) (employment, employment history, bank account number, or any other financial information)
- Commercial information (records of products and services purchased and other consumer history or tendencies)

- Internet or other electronic network activity information (browsing or search history, and information regarding consumer’s interaction with our websites)
- Geolocation data
- Inferences drawn from above information to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

We collect Personal Information directly from California residents and from data brokers, email service providers, social networks, and joint marketing partners. We do not collect all categories of Personal Information from each source.

In addition to the purposes stated above in the section “**Purposes and Legal Bases for Processing Personal Data**” we currently collect and have collected the above categories of Personal Information for the following business or commercial purposes:

- Helping to ensure security and integrity to the extent the use of your Personal Information is reasonably necessary and proportionate for these purposes
- Debugging to identify and repair errors that impair existing intended functionality
- Undertaking activities to verify or maintain the quality or safety of our products and services, and to improve, upgrade, or enhance our products and services

Sale, Sharing, and Disclosure of Personal Information

The following table identifies the categories of Personal Information that we disclosed for a business purpose in the 12 months preceding the last updated date of this Privacy Policy and, for each category, the categories of recipients to whom we disclosed Personal Information:

| Category of Personal Information | Categories of Recipients |
|---|---|
| Identifiers (name, postal address, email address, IP address, and other similar identifiers) | Operating systems and platforms; customer relationship management platforms; identity verification providers; regulatory bodies; government authorities; internet service providers |
| Personal information described in California’s Customer Records statute (California Civil Code § 1798.80(e)) (bank account number, credit card number, debit card number, or any other financial information) | Payment processor |
| Commercial information (records of products and services purchased and other consumer history or tendencies) | Operating systems and platforms; customer relationship management platforms; internet service providers |

| | |
|--|---|
| Internet or other electronic network activity information (browsing or search history, and information regarding consumer's interaction with our websites) | Operating systems and platforms; customer relationship management platforms; internet service providers |
| Geolocation data | Operating systems and platforms; customer relationship management platforms; internet service providers |

We disclosed Personal Information for the following business or commercial purposes:

- Helping to ensure security and integrity to the extent the use of your Personal Information is reasonably necessary and proportionate for these purposes
- Debugging to identify and repair errors that impair existing intended functionality
- Undertaking activities to verify or maintain the quality or safety of our products and services, and to improve, upgrade, or enhance our products and services

We have not sold or shared Personal Information in the twelve (12) months preceding the last updated date of this Privacy Policy. We do not collect, sell, or share the Personal Information of consumers under 16 years of age. We do not use sensitive Personal Information for purposes other than those allowed by the CCPA and its regulations.

Retention of Personal Information

We retain your Personal Information in accordance with Section 8 “Data Retention” above.

Your Rights

If you are a California resident you have the following rights with respect to your Personal Information:

- **Right to Opt-Out of Sale or Sharing:** you may request that we opt you out of the sale or sharing of your Personal Information. We do not currently sell or share your Personal Information.
- **Right to Know:** you may request disclosure about our collection of your Personal Information, including the categories of Personal Information, the categories of sources from which we collected Personal Information, the business or commercial purpose for collecting, selling, or sharing Personal Information (as applicable), the categories of third parties to whom we disclose Personal Information (if applicable), and the specific pieces of Personal information we collected about you.
- **Right to Request Deletion:** you may request that we delete Personal Information that we have collected from you, subject to certain exceptions.
- **Right to Non-Discrimination:** we will never discriminate against you by denying goods or services or providing a different level or quality of goods or services if you exercise any of these rights that have been granted to you.

- **Right to Correct Inaccuracies:** you may request that we correct inaccurate Personal Information that we maintain about you.
- **Right to Limited Usage:** if we use or disclose sensitive Personal Information for purposes other than those allowed by the CCPA and its regulations, you may request that we limit our use or disclosure of your Personal Information.

How to Submit a Request to Know, Delete, and/or Correct

You may submit a request to know, delete, and/or correct by calling us toll free at 1.800.480.0707 or by emailing us at privacy@netwitness.com.

How We Handle Your Requests

We will comply with your request upon verification of your identity, and, to the extent applicable, the identity of the California resident on whose behalf you are making such request. We will verify your identity either to a “reasonable degree of certainty” or a “reasonably high degree of certainty” depending on the sensitivity of the Personal Information and the risk of harm to you by unauthorized disclosure, deletion, or correction as applicable. To do so, we will ask you to verify date points based on information we have in our records concerning you.

Shine the Light Law

We do not disclose personal information obtained through our websites and services to third parties for their direct marketing purposes. Accordingly, we have no obligations under California Civil Code § 1798.83.

13. Changes to This Privacy Policy

We will update this Privacy Policy from time to time to reflect changes in our practices, technologies, and legal requirements.

If we make a material update, we may provide you with notice prior to the update taking effect by posting a notice on our websites or contacting you directly. We will seek your consent to these changes where required by applicable law if feasible.

We encourage you to periodically review this Privacy Policy to stay informed about our collection, processing, and sharing of your personal data.

14. COVID-19 Screening Tool and Thermal Vision Camera

In order to help reduce the risk of COVID-19 infections and keep our communities safe, all NetWitness employees, contingent workers, and visitors must complete a daily health survey and pass a thermal body temperature screening in order to gain access to NetWitness premises. The thermal vision camera measures your body temperature on an anonymous basis and RSA does not retain your body temperature. If your body

temperature is equal to or above 100 degrees Fahrenheit, you will be denied entry and/or asked to leave NetWitness premises.

The health survey screening tool, available via an app or web portal, collects your name, email address, and certain health data you voluntarily provide. This information will be retained on your device and not shared with RSA unless you self-report that you are COVID-19 positive. In that case, the tool will notify the appropriate RSA team, and your email address will be retained for up to 30 days (subject to local laws) so RSA may contact you as it takes appropriate action to protect the health and safety of individuals at RSA physical locations. Your COVID-19 positive status will be shared with the RSA team and applicable public health authorities (as required by law). Your status will also be shared on an anonymous basis with potentially infected individuals for contact tracing purposes.

15. Contacting Us

If you have questions about this Privacy Policy or our privacy practices, please email us at privacy@netwitness.com or write to us at:

NetWitness, a business unit of RSA Security LLC
Attention: Law Department – Privacy
2 Burlington Woods Drive Suite 201
Burlington, MA 01803 USA

Please be aware that your request may have limitations, according to applicable law.

Effective Date:

July 20, 2024.

Previous Privacy Policy:

- [September 20, 2022](#)

©2024 RSA Security LLC or its affiliates. All rights reserved. RSA Conference logo, RSA, NetWitness and other trademarks are trademarks of RSA Security LLC or its affiliates. Other trademarks may be trademarks of their respective owners.