

Trend Micro California Consumer Privacy Act Disclosures

Last updated: September 8, 2023

We, Trend Micro Incorporated, issue these California Consumer Privacy Act Disclosures (“**Disclosures**”) to provide information about how we collect, use, disclose and otherwise process California residents’ personal information and rights that California residents may have under the California Consumer Privacy Act of 2018 (“**CCPA**”). These Disclosures only apply to you if you reside in California. These Disclosures do not reflect our processing of California residents’ personal information where an exception under the CCPA applies.

1. Notice at Collection for Users of our Products

We collect the following categories of personal information about California residents who use our products and services (“**Users**”) for the following purposes:

- **User Activation and Contact Information:** Upon ordering, purchasing, installing, activating or using our products, we receive the following categories of personal information:
 - Name
 - Phone number
 - Email address
 - Device ID of the User’s device
 - Type of operating system that the User uses
 - License key for our product

These categories of personal information correspond with the categories identifiers, customer records and electronic information in the CCPA’s definition of personal information. We use this personal information to ensure that the relevant User’s license to our products is valid and to contact our Users regarding renewals, technical issues and new product information.

- **Product Usage Information:** We collect the following categories of information when California residents use and interact with our products and services, including customer support. The specific information that we collect will depend on the particular product or service that the User uses and can be found at [Data Collection Disclosure | Trend Micro Business Support](#) .
 - Product information, such as MAC address, device ID
 - Public IP address of the User’s gateway to the internet
 - Mobile/PC environment that the User uses
 - Metadata from suspicious executable files
 - URLs, domains and IP addresses of websites visited
 - Metadata of the User device managed by gateway product
 - Application behaviors

- Personal information contained within email content or files to which the User provides Trend Micro access
- Behaviors of Users
- Information from suspicious email to which the User provides Trend Micro access, including sender and receiver email address and attachments
- Detected malicious file information
- Detected malicious network connection information
- Debug logs
- Network architecture/topology
- Screen capture of errors

These categories of personal information correspond with the categories identifiers, customer records, Internet or other electronic activity information, and electronic information in the CCPA’s definition of personal information. We use these types of information to enable Users to participate, share and leverage our global database of threat-related intelligence to rapidly identify and defend against potential threats within Users’ network environments, as well as enabling us to provide any support requested.

We generally do not collect sensitive personal information from our Users unless they voluntarily provide it to us. Where permitted by law, we use all of the categories of personal information we collect to protect and secure our business operations, assets, online services, network, and information and technology resources; to investigate, prevent, detect and take action regarding fraud, unauthorized access, situations involving potential threats to the rights or safety of any person or third party, or other unauthorized activities or misconduct; to consider and undertake mergers, acquisitions or other business transactions that involve the sale of all or part of a business; to manage and respond to actual and potential legal disputes and claims; and to establish, defend or protect our rights or interests, including in the context of anticipated or actual litigation with third parties.

We do not sell Users’ personal information or share it for cross-context behavioral advertising. We retain Users’ personal information for as long as we have an ongoing legitimate business need to do so (for example, to provide a service the California resident has requested or to comply with applicable legal, tax or accounting requirements). When we have no ongoing legitimate business need to process a User’s personal information, we will either delete or pseudonymize it or, if this is not possible (for example, because their personal information has been stored in backup archives), then we will securely store that personal information until deletion is possible. Please find our California Consumer Privacy Act Privacy Policy below.

2. CCPA Privacy Policy

2.1 Our Personal Information Handling Practices over the Preceding 12 Months

The table below sets out the categories of “personal information” and “sensitive personal information” (as defined by the CCPA) that we collected from California residents over the preceding 12 months, their source, and to whom and for what purpose we disclosed the information. The table is followed by a description of the purposes for which we used such information about: (1) users of our products and services (“**Users**”); (2) representatives of our corporate customers and vendors (“**Business Contacts**”); and (3) our prospective, current and past employees and other personnel (“**Personnel**”). We do not “sell” or “share” personal information as the CCPA defines these terms.

Category of personal information	Did we collect? If so, from what source?	Did we disclose? If so, to whom and for what purpose?
Categories of “personal information” as defined in the CCPA		
Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.	Yes, directly from the California resident or from third-party sources such as distributors/reseller or partners	Yes, to our service providers and contractors to receive services from them
Any categories of personal information described in subdivision (e) of Section 1798.80; i.e., any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.	Yes, directly from the California resident or from third-party sources such as distributors/reseller or partners	Yes, to our service providers and contractors to receive services from them
Characteristics of protected classifications under California or federal law such as race, color, sex, age, religion, national origin, disability, citizenship status, and genetic information.	Yes, directly from the California resident	Yes, to our service providers and contractors to receive services from them
Commercial information including records of personal property, products or services purchased, obtained, or considered, or other purchasing or use histories or tendencies.	Yes, directly from the California resident	Yes, to our service providers and contractors to receive services from them

Category of personal information	Did we collect? If so, from what source?	Did we disclose? If so, to whom and for what purpose?
Categories of “personal information” as defined in the CCPA		
Biometric information.	No	Not Applicable (“N/A”)
Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement.	Yes, directly from the California resident	Yes, to our service providers and contractors to receive services from them
Geolocation data.	Yes, directly from the California resident	Yes, to our service providers and contractors to receive services from them
Audio, electronic, visual, thermal, olfactory, or similar information.	Yes, directly from the California resident	Yes, to our service providers and contractors to receive services from them
Professional or employment-related information.	Yes, directly from the California resident or from a third-party employment recruiter	Yes, to our service providers and contractors to receive services from them
Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).	Yes, directly from the California resident or from a third-party employment recruiter	Yes, to our service providers and contractors to receive services from them
Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	Yes, directly from the California resident, from a third-party employment recruiter, or their reference contacts, such as current and past employment managers	Yes, to our service providers and contractors to receive services from them
Categories of “sensitive personal information” as defined in the CCPA		
A California resident’s social security, driver’s license, state identification card, or passport number.	Yes, from Personnel themselves.	Yes, to our service providers and contractors to receive services from them

Category of personal information	Did we collect? If so, from what source?	Did we disclose? If so, to whom and for what purpose?
Categories of “personal information” as defined in the CCPA		
A California resident’s account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.	Yes, directly from the California resident	Yes, to our service providers and contractors to receive services from them
A California resident’s precise geolocation.	Yes, from Personnel themselves	Yes, to our service providers and contractors to receive services from them
A California resident’s racial or ethnic origin, religious or philosophical beliefs, or union membership.	Yes, from Personnel themselves	Yes, to our service providers and contractors to receive services from them
The contents of a California resident’s mail, email, and text messages unless the business is the intended recipient of the communication.	Yes, from Personnel themselves	Yes, to our service providers and contractors to receive services from them
A California resident’s genetic data.	No	N/A
The processing of biometric information for the purpose of uniquely identifying a California resident.	No	N/A
Personal information collected and analyzed concerning a California resident’s health.	Yes, from Personnel themselves	Yes, to our service providers and contractors to receive services from them
Personal information collected and analyzed concerning a California resident’s sex life or sexual orientation.	No	N/A

We use the personal information that we collect about **Users** for the following purposes: To ensure that the relevant User’s license to our products is valid to contact our Users regarding renewals, technical issues and new product information; and to enable Users to participate, share and leverage our global database of threat-related intelligence to rapidly identify and defend against potential threats within Users’ network environments, as well as enabling us to provide any support requested.

We use the personal information that we collect about **Business Contacts** for the following purposes: To provide our services; to develop, maintain and improve our services; to establish or administer our agreement with you or other request by you; to interact with you, including to communicate with you; to offer you content and services that might interest you, including newsletters, marketing, and promotional materials; and to comply with legal obligations, including responding to legal process or lawful requests .

We only use sensitive personal information that we collect about Users and Business Contacts for purposes referred to under Subsection 1798.121(a) of the CCPA or for purposes not subject to the CCPA, namely to: (i) perform the services or provide the goods reasonably expected by average California residents who request those goods or services; (ii) prevent, detect and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information; (iii) resist malicious, deceptive, fraudulent or illegal actions directed at us and to prosecute those responsible for those actions; (iv) perform services on behalf of us; (v) verify or maintain the quality or safety of our services and products; (vi) improve, upgrade, or enhance our services and products; and (vii) perform functions that are required under laws that apply to us.

We use the personal information that we collect about Personnel for the purposes set forth in our privacy notices at collection to Personnel. We only use sensitive personal information that we collect about Personnel for purposes referred to under Subsection 1798.121(a) of the CCPA or for purposes not subject to the CCPA, namely to:

- Perform the services or provide the goods reasonably expected by our Employees in their role as our Employees, including those services and goods that are reasonably necessary for us to initiate, administer or terminate the employment relationship and for our Employees to perform their duties;
- Prevent, detect or investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information, including in or via our premises, computers, software, networks, communications devices, and other similar system;
- Resist malicious, deceptive, fraudulent or illegal actions directed at us and to prosecute those responsible for those actions;
- Ensure the physical safety of natural persons;
- Short-term, transient use;
- Perform services on behalf of us;
- Verify or maintain the quality or safety of our services and products;
- Improve, upgrade, or enhance our services and products; and
- Perform functions that are required under laws that apply to us.

We use the personal information we collect about any California resident for the following purposes: To protect and secure our business operations, assets, online services, network, and information and technology resources; to investigate, prevent, detect and take action regarding fraud, unauthorized access, situations involving potential threats to the rights or safety of any person or third party, or other unauthorized activities or misconduct; to consider and undertake mergers, acquisitions or other business transactions that involve the sale of all or part of a business; to manage and respond to actual and potential legal disputes and claims; and to establish, defend or protect our rights or interests, including in the context of anticipated or actual litigation with third parties.

We do not have actual knowledge that we “sell” or “share” the personal information of California residents under 16 years of age, as “sell” and “share” are defined in the CCPA.

2.2 Your CCPA Rights

As a California resident, you have the following rights under the CCPA, subject to the conditions and exceptions set forth in the CCPA:

- The **right to know** what personal information we have collected about you, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom we disclose personal information, and the specific pieces of personal information we have collected about you. You may only exercise your right to know twice within a 12-month period.
- The **right to delete** personal information that we have collected from you.
- The **right to correct** inaccurate personal information that we maintain about you.
- The **right to opt-out of the sale or sharing** of your personal information by us. We do not “sell” or “share” personal information as the CCPA defines these terms.
- The **right not to receive discriminatory treatment** by the business for the exercise of privacy rights conferred by the CCPA, including an employee’s right not to be retaliated against for the exercise of their CCPA rights.

2.3 How to Exercise Your CCPA Rights

- **Methods of Submission and Instructions:** To submit a request to exercise your **rights to know, delete or correct**, please email privacy@trendmicro.com and specify in your request the details you would like to know, the information you would like deleted, or the information you would like corrected.
- **Verification:** Only you, or someone legally authorized to act on your behalf, may make a request related to your personal information. You may also make a request on behalf of your minor child. You may designate an authorized agent by taking the steps outlined under “Authorized Agent” further below. In your request or in response to us seeking additional information, you, or your authorized agent, must provide sufficient information to allow us to reasonably verify that you are, in fact, the person whose personal information was collected which will depend on your prior interactions with us and the sensitivity of the personal information being requested. We may ask you for information to verify your identity and, if you do not provide enough information for us to reasonably verify your identity, we will not be able to fulfill your request. We will only use the personal information you provide to us in a request for the purposes of verifying your identity and to fulfill your request.
- **Authorized Agents:** You can designate an authorized agent to make a request under the CCPA on your behalf if the authorized agent is a natural person or a business entity registered with the Secretary of State of California, we receive a written authorization stating that you have authorized the authorized agent to submit a request on your behalf which has been signed by you and the authorized agent, and we have verified the identity of you and the authorized agent. If you provide an authorized agent with power of attorney pursuant to California Probate Code sections 4121 to 4130, it may not be necessary to perform the above steps, and we will respond to any request from the authorized agent in accordance with the CCPA.

2.4 Contact for More Information

If you have questions or concerns regarding our privacy policy or practices, you may contact us using the following details: Email address: privacy@trendmicro.com Postal address: 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062.