

VERSION 2.4

Trustwave Privacy Policy

Table of Contents

TRUSTWAVE PRIVACY POLICY	1
Table of Contents	1
1 INTRODUCTION AND SCOPE	2
1.1 Introduction	2
1.2 Scope of Policy	2
2 PRIVACY PRACTICES	5
2.1 Personal Data Collected	5
2.2 Use of Personal Data	6
2.3 Sensitive Information	8
2.4 Disclosures	8
2.5 Opting Out / In	8
2.6 Rights of Data Subjects in the European Union / European Economic Area	9
2.7 Rights of Data Subjects Residing in the State of California, United States	9
2.8 Rights of Data Subjects in Australia	10
2.9 Security	10
2.10 Considerations on Data Erasure	10
2.11 Changes to this Privacy Policy	11
3 QUESTIONS, COMPLAINTS AND DISPUTE RESOLUTION	12
3.1 Contact Details	12
3.2 Privacy Shield Dispute Resolution for Data Subjects in the European Union / European Economic Area	13

1 Introduction and Scope

1.1 Introduction

Trustwave Holdings, Inc., a company incorporated in the USA whose registered office is at 70 W. Madison St., Suite 600, Chicago IL 60602.

Trustwave Holdings, Inc., its parent company, its subsidiaries and its related companies (together “**Trustwave**”, “**we**”, “**us**”, “**our**”), are committed to maintaining the privacy, security, and accuracy of your personal data. As a result, Trustwave has developed this policy to inform you of the steps it has taken to protect your privacy. In addition, Trustwave and its employees also adhere to strict internal information security policies and procedures to safeguard your information. For more information about which subsidiaries are covered by this policy, please see the “*Scope of Policy*” section below.

Trustwave complies with all applicable data protection laws, including, without limitation, the General Data Protection Regulation (“GDPR”), the California Consumer Privacy Act (“CCPA”), and the Privacy Act 1988 (Cth) (“Privacy Act”).

Trustwave also complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data transferred from the European Union and the United Kingdom to the United States (the “**Privacy Shield**”). Trustwave Holdings, Inc. has certified to the Department of Commerce that it adheres to the Privacy Shield Principles (the “**Principles**”). If there is any conflict between the terms in this privacy policy and the Principles, the Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>.

The Federal Trade Commission and/or the Department of Transportation have jurisdiction over Trustwave Holdings, Inc.’s and its subsidiaries’ compliance with the Privacy Shield.

1.2 Scope of Policy

This policy and Trustwave’s Privacy Shield certification cover personal data that is transferred from the European Economic Area to Trustwave Holdings, Inc. and the following entities:

TRUSTWAVE LIMITED
TRUSTWAVE GERMANY GMBH
TRUSTWAVE SWEDEN AB
TRUSTWAVE POLAND SP. Z. O. O.
BREACH SECURITY, LTD.
M86 INTERNATIONAL LTD.
M86 SECURITY AUSTRALIA LTD.
M86 SECURITY AUSTRALIA PTY LTD.
M86 SECURITY ISRAEL, LTD.
M86 SECURITY NZ LIMITED
M86 TAIWAN (BRANCH OF M86 AMERICAS, INC.)

SERVICIOS TECNOLOGICOS TRUSTWAVE CHILE LIMITADA
TRUSTWAVE CANADA, INC.
TRUSTWAVE COLOMBIA SUCURSAL DE SOCIEDAD EXTRANJERA (BRANCH OF TRUSTWAVE BRAZIL)
TRUSTWAVE DO BRASIL SEGURANCA DA INFORMACAO E CONFORMIDADE LIMITADA
TRUSTWAVE INFORMATION SECURITY AND COMPLIANCE INDIA PRIVATE LIMITED
TRUSTWAVE JAPAN CO., LIMITED
TRUSTWAVE MÉXICO SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE
TRUSTWAVE PHILIPPINES INC.
TRUSTWAVE PTE. LTD.
TRUSTWAVE SECURITY SOLUTIONS PROPRIETARY LTD
TW ASIA PACIFIC LIMITED
TWH AUSTRALIA PTY. LTD.
OPTUS CYBER SECURITY PTY. LTD.
SINGTEL CYBER SECURITY PTY. LTD.
SECURETRUST, INC.
SECURETRUST COMPLIANCE LTD.

This Policy also covers personal data from California and Australian residents that is collected and/or shared by Trustwave. Additional information on California and Australian residents' rights required under the CCPA and the Privacy Act may be found in the "*Rights of Data Subjects Residing in the State of California, United States*" and "*Rights of Data Subjects in Australia*" sections below. References to 'personal data' throughout this Policy shall have their meaning derived from the relevant terminology and definitions set forth by the applicable law.

In general, Trustwave may share your personal data with any member of the subsidiaries listed above who may process your personal data for the purposes specified in this privacy policy. The list of Trustwave companies with whom your data may be shared will change from time to time, so please ensure that you revisit this policy regularly.

Because Trustwave respects your right to privacy, it has implemented privacy practices in the provision of its services, products, and website, including in accordance with the Privacy Shield, GDPR, the Australian Privacy Principles ("APPs") and other applicable law.

For individuals specifically located in the European Economic Area, Trustwave commits to complying with the following Principles in respect of all personal data which is received from individuals based in the European Union and transferred to the United States of America and other Trustwave subsidiaries:

1. **Notice:** Trustwave is committed to providing you with information about its participation in and responsibilities under the Privacy Shield, the types of information that Trustwave may collect from you and how they are used, your rights in relation to your personal data, and how to contact Trustwave and/or the available independent dispute resolution body designated to address complaints;
2. **Choice:** Where possible, Trustwave will allow you to opt out of (i) disclosures of your personal data to third parties; or (ii) use of your personal data for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by you;
3. **Accountability for Onward Transfers:** Trustwave will only transfer your personal data to third parties where: (i) such transfer is only for limited and specified purposes; (ii) the third party provides at least the same level of privacy protection as the Principles; (iii) the processing is consistent with Trustwave’s obligations under the Principles; (iv) the third party is required to notify Trustwave if it can no longer provide sufficient protection for your personal data; (v) the third party takes steps to stop and remediate unauthorized processing; and (vi) Trustwave commits to provide a summary of the relevant privacy protections in place with that third party to the Federal Trade Commission upon request;
4. **Security:** Trustwave will take reasonable and appropriate measures to protect personal data from loss, misuse or unauthorized access, disclosure, alteration or destruction;
5. **Data Integrity and Purpose Limitation:** Trustwave will take steps to limit the personal data that it processes about you to that which is relevant for the purposes of processing. Trustwave will also take steps to hold the data it processes about you for as long as it serves the purpose of processing. Trustwave will also take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current;
6. **Access:** You have a right to access the personal data that Trustwave holds about you and to correct, amend, or delete that information where it is inaccurate or has been processed in violation of the Principles; and
7. **Recourse, Enforcement and Liability:** Trustwave provides robust mechanisms for assuring compliance with the Principles and recourse for individuals who are affected by non-compliance with the Principles. Further details on the recourse mechanisms available to you can be found under the “*Recourse and Dispute Resolution*” section below.
8. **Lawful basis of processing:** Trustwave will process personal data on the basis of consent, out of necessity for the performance of a contract, legitimate interests for marketing purposes, and to protect our legal position in the event of legal proceedings.

2 Privacy Practices

2.1 Personal Data Collected

In general, you can access Trustwave’s website(s) and use its services without giving us any personal data. However, many of Trustwave’s products, services and interactions with you will involve the collection of various “personal data” about you which are explained in detail below. Personal data is information which can identify you as a living individual when used in isolation or in conjunction with other information.

In addition to any information you voluntarily provide to us or input through Trustwave’s website(s), we may collect the information in the following circumstances:

Products / Services. Trustwave may collect your personal data in connection with providing you with services and/or products. The specific types of personal data collected from you is dependent on the services or products you select but this information may include:

- full name;
- contact details including address, phone numbers and email address;
- job role and employer name;
- bank account information including credit card number;
- tax identification number; and
- second-level domain information and IP addresses
- commercial information such as products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies records

If you select to enroll for an SSL certificate, you will be required to provide Trustwave with certain personal data as set forth in Trustwave’s Certification Practices Statement, which may be found at <https://certs.securetrust.com/CA/>. It is important to note that Trustwave is requesting this information for the purpose of authenticating your identity to create and issue your SSL certificate.

Partners. Trustwave may also obtain your personal data from third parties, such as partners and resellers, but only to the extent it is required to provide you with our products and/or services. This information may include:

- full name;
- contact details including address, phone numbers and email address; and
- bank account information including credit card number.

Website and Subscriptions. Other than during your enrollment for services and/or products, Trustwave also collects personal data from you if you access Trustwave’s website(s) and/or you choose to register for events, subscribe to email listings throughout our website, request that we contact you, or apply for a job opening at the company. This information may include:

- full name;
- contact details including address, phone numbers and email address as well employment and educational history (if you apply for an open position);
- second-level domain information and IP addresses;
- information gathered from cookies (see “*Cookies*” section below).

Cookies. Trustwave also utilizes cookies when you visit its website(s), or during the use of its products, which is a piece of data used by web servers to help identify you. A cookie is installed automatically when you use the site but you can reject or disable a cookie by changing a setting on your browser. Trustwave uses session, non-persistent cookies to help offer you secure pages to our website that allow you to login automatically across sessions. A list of our cookies can be provided on request in accordance with the “Contact Details” section.

2.2 Use of Personal Data

Trustwave may use your personal data as follows:

- Where collected in connection with our products and services:
 - to provide you with products, services and any renewals thereof;
 - to provide you with support and maintenance for products/services;
 - to inform you of any new or updated services or product offerings;
 - to bill you for products and services;
 - to notify you of any changes to your use of our website, products, or services;
 - to respond to your enquiries;
 - to have a partner or independent reseller contact you to facilitate the renewal, support or purchase of products/services, but only to the extent such third party has executed a confidentiality agreement with obligations to protect your personal data (for a list of these third parties, please contact us at the address set forth at the end of this policy);
 - to authenticate your identity in order to provide you with an SSL certificate (your personal data may be provided to an independent third party resource for verification);
 - to issue you an SSL certificate, some of your personal data will be published within the certificate itself or in Trustwave’s SSL certificate repository as set forth in our Certification Practices Statement. Publication of such information is germane to the widespread use of SSL certificates;
 - to transfer or negotiate the transfer of ownership of Trustwave or its assets during any merger, acquisition or sale, even if they are not in the same line of business as us (in such event, your personal data will be held subject to this Privacy Policy); and
 - to comply with applicable law and law enforcement authorities.
- Where collected from third parties:
 - to provide you with products, services and any renewals thereof;
 - to provide you with support and maintenance for products/services;
 - to inform you of any new or updated services or product offerings;

- to bill you for products and services;
 - to notify you of any changes to your use of our website, products, or services;
 - to respond to your enquiries;
 - to have a partner or independent reseller contact you to facilitate the renewal, support or purchase of products/services, but only to the extent such third party has executed a confidentiality agreement with obligations to protect your personal data (for a list of these third parties, please contact us at the address set forth at the end of this policy);
 - to authenticate your identity in order to provide you with an SSL certificate (your personal data may be provided to an independent third party resource for verification);
 - to issue you an SSL certificate, some of your personal data will be published within the certificate itself or in Trustwave's SSL certificate repository as set forth in our Certification Practices Statement. Publication of such information is germane to the widespread use of SSL certificates;
 - to transfer ownership of Trustwave during any merger, acquisition, or sale (in such event, your personal data will be held to the same confidentiality obligations); and
 - to comply with applicable law and law enforcement authorities.
- Where collected in connection with your access to Trustwave's website(s) and/or you registering for events, subscribing to email listings, requesting that we contact you or applying for a job opening:
 - to inform you of any new or updated services or product offerings;
 - to notify you of any changes to your use of our website, products, or services;
 - to analyze the use of our website to improve its layout and services;
 - to respond to your enquiries;
 - to review your candidacy for a job opening at the company;
 - to transfer ownership of Trustwave during any merger, acquisition, or sale (in such event, your personal data will be held to the same confidentiality obligations); and
 - to comply with applicable law and law enforcement authorities.

The uses listed above are not intended to be exhaustive and may be updated from time to time as business needs and legal requirements dictate. Where appropriate, you will be given a more detailed explanation as to how your personal data is used on a case by case basis.

Trustwave's website(s) may link to other websites which are not within its control. Once you have left Trustwave's website(s), Trustwave cannot be responsible for the protection and privacy of any information which you provide. You should exercise caution and look at the privacy statement applicable to the website in question.

2.3 Sensitive Information

Information about you which is considered sensitive or a special category of personal data under data protection laws can include information about your medical or health conditions, racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, genetic data, biometric data, sexual life and sexual orientation, and suspected or proven criminal activity and related proceedings. If we need to process sensitive or special categories of personal data, you will be notified of such processing and asked to specifically agree to the use of such information as appropriate.

Trustwave asks that you do not provide any sensitive or special categories of personal data unless Trustwave specifically asks for this.

2.4 Disclosures

Trustwave may share your personal data with any of its subsidiaries, related companies or parent who may process your personal data for the purposes specified in this privacy policy.

Sometimes Trustwave will share your information with carefully selected third parties outside of Trustwave's corporate group (such as its partners, resellers, and subcontractors, such as service providers, Internet cookie information recipients, advertisers, social media companies). Trustwave may do this for the following reasons:

- To carry out services for Trustwave;
- To provide you with information about special promotions and offers which we think you might be interested in;
- In response to lawful requests by public authorities, including to meet national security or law enforcement requirements;
- When Trustwave believes it is necessary to comply with the law or protect our or another person's rights, property, or safety; and/or
- If there is (or is to be) any change in ownership of any Trustwave business or assets then Trustwave may wish to share your information so that the new (prospective) owners may continue to operate our business effectively and continue to provide services to customers. This may include new shareholders or any organization that might take an assignment or transfer of any agreements we have entered into with Trustwave's customers.

Trustwave will place appropriate obligations and restrictions on third parties to protect your details.

Trustwave will remain responsible to you under the Principles in the event any of its agents processes your personal data in a manner inconsistent with the Principles except where Trustwave can prove that it is not responsible for the relevant event.

Some Trustwave companies, and sometimes other third parties with whom we share personal data are or may be located outside your country of origin.

2.5 Opting Out / In

If you are a customer or you have previously asked us for information on Trustwave's products and/or services, Trustwave may send you information on its range of products and services to your contact details, unless you have asked us not to do so.

You may opt out of having your personal data used for marketing purposes and/or any purpose inconsistent with the purpose it was originally collected or authorized by you. Please contact

marketing@trustwave.com or visit https://www2.trustwave.com/preference_center.html to opt-out or change your preference.

If you receive marketing material from our partners or other third parties, and no longer wish to receive such material, you must opt-out directly with that party.

2.6 Rights of Data Subjects in the European Union / European Economic Area

At any time, you may have access to your personal data for any reason, including without limitation reviewing, correcting, deleting inaccuracies or updating such information by sending a request to Trustwave in accordance with the “*Contact Details*” section below. You may also have the right to erase your personal data, restrict the processing, the right of portability and the right to object to the processing in certain circumstances. Where appropriate, Trustwave will verify your identity before processing any requests. European data subjects requesting erasure of their personal data must also review the “*Considerations on Data Erasure*” section below.

2.7 Rights of Data Subjects Residing in the State of California, United States

Effective January 1, 2020 and unless otherwise stated in this policy, the practices and activities detailed herein also apply to you if you were considered to be a California resident during the collection of your personal data. As a California resident, you may have:

- (1) the right to know the categories of personal data that may be collected about you and related categories of sources for collection in addition to the business purposes for which that information would be used or shared;
- (2) the right to know the categories and specific pieces of personal data that were collected or shared for business purposes about you in the preceding 12 months of your request;
- (3) the right to know the categories of third parties with whom your personal data was shared;
- (4) the right to delete your personal data; and
- (5) the right to not be discriminated against if you choose to exercise your privacy rights.

You may inform us that you want to exercise your rights in accordance with the “*Contact Details*” section below. Trustwave will verify your identity before processing any requests and you are entitled to make such request no more than twice in a 12-month period. Please also note that the CCPA contemplates certain exemptions or exceptions for certain types of transactions or other reasons contemplated by law. If you contact Trustwave regarding your personal data and an exemption or exception applies, we will inform you of that fact. California residents requesting erasure of their personal data must also review the “*Considerations on Data Erasure*” section below.

Businesses are also required to disclose whether they sell personal data to third parties. Trustwave does not sell your personal data.

For additional information on (a) the categories of personal data we collect about you and their sources, (b) how we use this information, and (c) how this information may be shared with third parties, please consult Sections 2.1, 2.2, and 2.4 of the “*Privacy Practices*” section above.

2.8 Rights of Data Subjects in Australia

Trustwave abides by the APPs, which provide a scheme in relation to the collection, disclosure, use and storage of personal data.

Collection of Personal Data. Where lawful and practicable (i.e. if we are still able to provide the relevant service or information to you without your information), you may choose to deal with Trustwave anonymously or under a pseudonym.

International Transfer of Personal Data. Generally, your personal data is likely to be stored in Australia. However, some Trustwave companies and service providers are located overseas, and in some instances, your personal data may be transferred to or processed by Trustwave companies and service providers in overseas countries, including but limited to the United States and Singapore.

If there is an international transfer of personal data (whether by disclosing it to such parties or merely by allowing them to access it) we will take appropriate steps to ensure that it is carried out in accordance with the applicable privacy laws and the AAPs. If you have any questions about the collection, use, disclosure, or storage of your personal data, please contact us using the details at the “*Contact Details*” section below.

Access to your Personal Data. You may request details related to the personal data that we hold about you in accordance with the provisions of the Privacy Act. If you would like a copy of the information which we hold about you or believe that any information we hold on you is inaccurate, out of date, incomplete, irrelevant or misleading, you may send a request to Trustwave in accordance with the “*Contact Details*” section below.

Additionally, if you have a complaint about our privacy practices, please submit the details of your complaint in accordance with the “*Contact Details*” section below. Please note that your complaint must be made in writing as required by section 40(1A) and that we will respond within a reasonable time as determined by the Privacy Act.

2.9 Security

Trustwave utilizes appropriate technical and organizational measures to ensure that the confidentiality, integrity and availability of our systems and services protect your personal data. We take all reasonable steps to ensure that the personal data we hold is protected from misuse, interference, and loss, and unauthorised access, modification or disclosure by the use of various methods, including secure storage.

2.10 Considerations on Data Erasure

When processing a valid request for erasure of personal data in accordance with this privacy policy and applicable law, Trustwave will promptly erase personal data from live systems based on the scope defined between the parties. Where data erasure applies to you, please also consider the following:

- Depending on the extent of your relationship with Trustwave, your data may be retained in Trustwave’s backup systems for a longer period of time in a format that is beyond use;
- Backup systems play a crucial role in Trustwave’s data security program and in ensuring the availability and access to data in a timely manner in the event of a physical or technical incident;
- Data erasure on certain backup systems may not be immediately possible due to existing technical controls designed to keep information temporarily available to Trustwave’s information technology team solely when fully required in the event of a physical or technical incident;
- Relevant data retained in certain backup systems will not be used for any other purpose and will be secured with the appropriate technical and organizational measures based on the requirements of data protection law; and
- Relevant data retained in backup systems will be kept until such data is overwritten and completely erased based on Trustwave’s internal backup retention schedule and policies.

Trustwave will provide information where these considerations apply on a case-by-case basis.

2.11 Changes to this Privacy Policy

Trustwave may amend this privacy policy from time to time. If any amendments are made, then a notice will be posted on Trustwave’s website. This privacy policy was last updated on 31 August 2020.

3 Questions, Complaints and Dispute Resolution

3.1 Contact Details

All inquiries, questions and complaints regarding how Trustwave processes your personal data and/or this privacy policy may be sent to Trustwave's Privacy Department:

E-mail: dataprotection@trustwave.com

Postal Address:

Attention: Privacy Department		
Trustwave Holdings, Inc.	Trustwave Limited	Optus Cyber Security Pty Ltd
70 W. Madison St.,	3 Albert Embankment	Level 11, 309 George St
Suite 600	Westminster Tower	
Chicago, IL 60602,	SE1 7SP London	Sydney, NSW 2000
United States of America	United Kingdom	Australia

You may also choose to submit your request through our privacy inquiry form found here: <https://privacyportal-cdn.onetrust.com/dsarwebform/cfc2078e-161f-4759-b77f-97e1819dc857/a293e68f-21d9-467d-abf2-491c775dd32d.html>.

Trustwave will promptly respond to all enquiries and implement a corrective course of action, if necessary.

3.2 Privacy Shield Dispute Resolution for Data Subjects in the European Union / European Economic Area

In compliance with the Privacy Shield Principles, Trustwave commits to resolve complaints about our collection or use of your personal data. European Union individuals with enquiries or complaints regarding our Privacy Shield policy should first contact Trustwave at: dataprotection@trustwave.com

Trustwave has further committed to refer unresolved Privacy Shield complaints to JAMS International (“JAMS”), an alternative dispute resolution provider located in London, England. If you do not receive timely acknowledgment of your complaint from us, or if we have not resolved your complaint, please contact or visit JAMS at <https://www.jamsinternational.com/> for more information or to file a complaint. The services of JAMS are provided at no cost to you.

Trustwave also commits to cooperate with the panel established by the EU data protection authorities (“DPAs”) and comply with the advice given by the panel with regard to personal human resources (HR) data transferred from the European Union.

Under certain conditions, you have a right to invoke binding arbitration for complaints regarding Trustwave’s Privacy Shield compliance not resolved by under the dispute resolution mechanism set out above. For additional information regarding binding arbitration, please see: <https://www.privacyshield.gov/article?id=ANNEX-I-introduction>.

Last amended: 31 August 2020