JEFFERSON INSURANCE COMPANY
(A Stock Company)

NEW JERSEY STATE AMENDMENT

Your policy is changed as follows:

1. **GENERAL PROVISIONS AND CONDITIONS**, Proof of Loss provision is revised by adding the following:

   All benefits will be paid within 30 days after receipt of complete proof of *your* loss.

There are no other changes to *your policy*.

Jefferson Insurance Company

Elena Edwards, President

IMPORTANT PRIVACY NOTICE

THIS NOTICE DESCRIBES HOW PERSONAL DATA AND MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN ACCESS THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

AWP USA Inc. and its subsidiaries, including Jefferson Insurance Company and AGA Service Company d/b/a Allianz Global Assistance are committed to protecting your privacy. By using our products, services or website, you consent to our collection and use of your Personal Data as described in this notice ("Notice").

Definitions. The below definitions apply to this Notice:

1. "Personal Data" means non-public personal information that identifies a specific identified or identifiable person ("you"). An identifiable person is one who can be identified by reference to an identifier (such as name) or other factors specific to that person. Personal Data does not include publicly available, de-identified, or aggregated data.

2. "Sensitive Data" means Personal Data about a person's race or ethnicity; political, religious, philosophical, ideological, or trade union memberships, opinions, views or activities; medical or health conditions or protected health information ("PHI") as defined in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); genetic or biometric data; financial account information (e.g. bank account number); government-issued ID numbers; sexuality; or social security measures or administrative or criminal proceedings and sanctions that are treated outside pending proceedings. Sensitive Data also includes information we receive from a third party who treats and notes the information as sensitive.

3. "Agent" means a third party that collects or uses Personal Data to perform tasks on our behalf, or our underwriters.

4. "We/Us/Our" means one or more of AWP USA Inc., Jefferson Insurance Company and AGA Service Company.

Privacy Practices. This Notice describes how we collect, use, and maintain Personal Data. It also describes your and our rights.

For the Personal Data of EU and Swiss residents, we comply with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States, respectively (collectively, the "Privacy Shield"). We have certified to the Department of Commerce that we adhere to the Privacy Shield Principles regarding EU and Swiss Personal Data received under the Privacy Shield. If there is any conflict between the terms in this Notice and the Privacy Shield Principles, the Privacy Shield Principles shall govern in matters regarding EU and Swiss residents. To learn more about the Privacy Shield and to view our certification, visit https://www.privacyshield.gov.

1. Notice: We collect Personal Data from you, or from your agents, representatives, suppliers and providers, or other party from whom you have authorized us to collect it on your behalf. This may include:
   (i) Identifiers and other identifying personal information (e.g. name, contact information like address, email address, or other unique personal identifiers, signature, date of birth, insurance policy numbers, education, employment information and history);
   (ii) billing or payment information (e.g. bank account or payment card number and billing information);
   (iii) information about your trip, event, or enrollment (e.g. agents, suppliers, trip itinerary and plans; tuition and enrollment information);
   (iv) information about your transactions or business with us or others (e.g. personal information you provide us for us to generate quotes or to purchase products, quote/purchase history, receipts, insurance EOBs);
   (v) financial account information (e.g. account numbers, statements);
   (vi) health information (e.g. health insurance information, disability information, medical treatment history, invoices);
   (vii) information about or related to any claim you make or other use of our products (e.g. details of your loss, police reports, health/vital records, professional or employment-related information) records of interactions, communications and correspondence between you and us, including audio and electronic information);
   (viii) information about your websites and/or mobile application (e.g. browser data, IP address, information about your interaction with a website, application, or advertisement);
   (ix) geolocation data (e.g. for use of location-based website or mobile application customization or services);
   (x) biometric information (e.g. fingerprinting required for insurance licenses);
   (xi) protected class information (e.g. age, which may be used for purposes of quoting, or disability which may be used in administration of your claim)
   (xii) government-issued identification numbers (e.g. social security number, driver's license number, passport number); or

(xiii) any other information provided to us by you or on your behalf.

We may also collect Personal Data from consumer reporting agencies or fraud databases (e.g. fraud reports). This data may be collected from forms, such as enrollment or claim forms; by phone, website, email, fax, or correspondence; or via cookies.

We may use the Personal Data we collect from any of the above categories to:
(i) to offer, market, sell, underwrite, or make available to you insurance or assistance products or services;
(ii) to provide you with information or services for such products and services;
(iii) to service and administer your insurance, assistance, or other products and services. This may include, for example: providing travel assistance or concierge services, servicing and processing your policy or claims, conducting quality or satisfaction surveys and assessments, keeping electronic or audio records of our interactions and correspondence with you and documents sent and received; and fraud prevention;
(iv) to arrange for the provision of services you request;
(v) to protect our legal rights or to respond to lawful requests by public authorities, including to meet national security or law enforcement requirements or as otherwise required by law; or
(vi) for purposes to which you've otherwise consented.

This may in some cases include disclosing your Personal Data to Agents. But, such disclosures are only for the purposes described in this Notice, or for everyday business purposes or as required or allowed by law (e.g. to process transactions, maintain accounts, respond to court orders and legal investigations, or report to credit bureaus). These Agents may be affiliated or nonaffiliated, and may be located both inside and outside of the US. They may be financial services providers (e.g. underwriting insurers). They may also be non-financial companies (e.g. health service providers, travel service providers, the agent/agency through whom you purchased, service providers helping us with marketing or technology).

Should you be purchasing insurance on another's behalf, we and the insurer may require the personal information of the insured to provide and administer the benefits of their plan. By providing the insured's personal information at the time of purchase, you are confirming that you have obtained the insured's consent to provide this personal information for this use.

Where we are subject to HIPAA, we must notify you of our duties and practices with respect to PHI. Except as described here or allowed or required by law, we will only use or disclose your PHI or health records with your prior express consent. Under HIPAA, we may use and disclose your PHI for one or more of the following purposes:
(i) monitoring the health care treatment you receive (e.g. we may send or receive PHI to or from a doctor regarding your condition and treatment so we can see that your treatment is appropriate);
(ii) payment for health services (e.g. we may use your PHI to make payments to a hospital that has treated you);
(iii) to help run our company (e.g. we may use your PHI to conduct quality audits of the services we provided to you. However, we may not use or disclose genetic information about you for underwriting purposes); or
(iv) for other purposes as required to administer your insurance or assistance product (e.g. we may use PHI to determine coverage for a claim made under an insurance policy).

We may also in some cases need to use or disclose information about you which may include your PHI for one or more of the following purposes:
(i) for public health and safety issues;
(ii) to comply with legal or regulatory requirements;
(iii) to address or comply with workers' compensation, law enforcement, or other legal or government mandates or requests; or
(iv) to respond to lawsuits or legal actions.

Cookies are text files on your computer. When you access our website or use our mobile application, we use cookies, among other things, to collect data about your web usage. We also use Google, Inc.'s Google Analytics and AdWords services, iAdvize and Jacada's chat and monitoring service, and other similar third-party vendor services. These services use cookies to transmit your IP address and other website navigation and Internet usage/network activity data and device/browser-generated data, including regarding your browsing history and your interaction with our and other websites, applications, and advertisements. iAdvize also uses JavaScript to provide its chat and monitoring services. These vendors may provide this data to us or store and/or aggregate this data to analyze such usage and create reports for us. We, our affiliates and our Agents use such data and reports for our own business purposes (e.g. to provide customer service, to optimize the content you see from us, website improvement, other purposes stated in this Notice, etc.) and Payment Card Industry Data Security Standard ("PCI") compliance. These vendors may also display our ads on sites across the Internet, and they may use this data to later display ads or other

information to you based on your website usage or other information collected as described above. By using our website, you consent to this use of cookies and data for these purposes. You can refuse cookies by disabling them in your browser (this may affect the content available to you). Our websites do not respond to "Do Not Track" requests from browsers.

We may use your geolocation information for generating location-specific product advertisements and offers or to provide and administer the insurance and assistance services as described above. This information may also be used for location-based website or mobile website application services, such as access to local alerts and emergency services numbers and providers, maps, and translation services, and other similar services, or for purposes to which you otherwise consent or as described here.

Last, we may use and disclose the name, email address, or contact information of current and former customers to Agents for marketing administration purposes. For example, we may need to disclose the email address you provided to us to an Agent providing marketing services on our behalf to help ensure that your opt out choices are respected and that you do not receive duplicate communications.

Upon notification and consent your personal data may be used for other reasons. That notice will state the purpose for collecting and using the data, the types of non-Agent third parties to which we disclose the data, and the means we offer you to limit this. If we receive Personal Data from anyone in the EU or Switzerland, we'll treat that data according to the instructions such entity gives us regarding notices it provided and the choices made by the data subject.

2. Choice. We reserve the right to disclose Personal Data to third parties as described above. The law in some jurisdictions allows you the right to choose in some cases to opt out of us sharing your Personal Data with a third party or using it for purposes described or that is materially different from the purposes for which it was originally collected or which you later authorize. You may exercise this right by notifying the Privacy Officer at the information provided below. You may opt out of getting non-essential marketing communications from us by giving notice as described below and disabling cookies in your web browser. Except as required or allowed by law (e.g. for fraud prevention), we do not share, sell or otherwise disclose your Personal Data to non-Agent third parties or use it for any purpose other than for which it was originally collected or as you later authorize. If we ever wish to do so, we will give you the opportunity to opt out. If we wish to disclose your Sensitive Data to a non-Agent third party or use such data for a purpose other than for which it was originally collected or as you later authorize, we will only do so with your express consent. We will not unfairly discriminate against you for declining to provide this consent.

   Except as allowed by law, we will not use or disclose psychotherapy notes, use or disclose your PHI for marketing purposes, or use or disclose your PHI in a way that would constitute a sale of PHI under HIPAA unless you expressly authorize us to do so. You may revoke this consent at any time. Such revocation will not apply to actions we have already taken based on that consent. You may request restrictions on our use and disclosure of certain health information for treatment, payment, or our operations. However, we are not required to agree to your request, except as required by HIPAA.

   We may need to disclose Personal or Sensitive Data if we have a good-faith belief that it is needed to protect or defend our or your rights, interests or property or comply with any law or legal mandate, or if it is otherwise required or allowed by law. We will take reasonable care to disclose only as much of such data as is needed.

3. Accountability for Onward Transfer. We may disclose your Personal Data to our Agents, but only for the limited and specified purposes described here, consistent with the consent you have provided. We will take reasonable and appropriate steps to obtain assurances from our Agents that they will effectively process and safeguard your Personal Data consistent with our obligations under this Notice and the Privacy Shield (EU and Swiss residents only). Upon discovery, we will take reasonable steps to stop and remediate any unauthorized processing inconsistent with this Notice or the Privacy Shield (EU and Swiss residents only). With respect to EU or Swiss Personal Data we receive under the Privacy Shield and later transfer to an Agent, we are responsible for the processing of such data by that Agent. If such data is processed by that Agent in a manner inconsistent with the Privacy Shield Principles, we are liable unless it can be proved that we are not responsible for the event giving rise to any damages.

   Our Binding Corporate Rules related to data transfers may be viewed here: https://www.allianz-partners.com/en_US/allianz-partners---binding-corporate-rules-.html

4. Security. We take reasonable and appropriate measures to protect your data from loss, misuse, or unauthorized access, disclosure, alteration and destruction. These measures take into account the risks involved in the processing and the nature of the Personal Data. To help maintain the security of your data, we use administrative, physical, and technical safeguards. These include utilizing policies to take reasonable precautions to (a) securely and confidentially

maintain your Personal Data; (b) assess and protect against threats and hazards to the security or integrity of such data; and (c) prevent unauthorized access to or use of such data. Also, except where required or allowed by law, we limit use of your Personal Data to the minimum necessary to accomplish the purposes for which that data was collected and to be used as described here. We restrict access to your Personal Data to only those who need to access it to accomplish those purposes. We use encryption to make your online transaction with us safe and secure. We protect the privacy of your credit card information with a high degree of care and in compliance with PCI. We are required by law to maintain the privacy and security of your PHI. If there is a breach as defined under HIPAA of your unsecured PHI, we are required by law to notify you.

5. Data Integrity. We will only collect Personal Data to the extent it is relevant to the purposes for which it was collected. We will not process Personal Data in a way that is incompatible with the purposes for which it has been collected or as you later authorize. To help maintain the integrity of your data, we will take reasonable steps to ensure that Personal Data is reliable for its intended use, relevant, accurate, complete, and current. We will adhere to these principles for as long as we retain this data. We retain Personal Data according to our data retention policy.

6. Access. If you discover the data we hold about you is inaccurate or incomplete, please contact us. We will grant you reasonable access to the Personal Data we hold about you. We will take reasonable steps to allow you to correct, amend or delete your Personal Data that is inaccurate or incomplete, or has been processed in violation of this Notice, so long as it can be done without undue burden or expense on us, without breaching any legal or professional privilege or obligation, and without violating the rights of others. Where we are subject to HIPAA, you have the right to request to receive confidential communications of your PHI, as applicable. In accordance with and as allowed by HIPAA, at your request, you may inspect, amend, and copy PHI we maintain about you and receive an accounting of certain disclosures of your PHI (e.g. health payment records).

7. Recourse, Enforcement, Liability. You can send complaints about how we handle your Personal Data to us at the contact information below. If the data is PHI, complaints can be made to us or to the U.S. Secretary of Health and Human Services. We will not retaliate against you for filing a complaint. For EU and Swiss Personal Data, we verify our compliance with the Privacy Shield and the terms of this Notice by conducting a periodic self-assessment. Complaints or disputes about how we handle EU or Swiss Personal Data should be directed to the below address. We will promptly investigate and try to resolve any such complaints or disputes internally. But, if we can't reach a mutually agreeable resolution, we have agreed to cooperate with the dispute resolution procedures administered by, as applicable, the European Data Protection Authorities or the Swiss Federal Data Protection and Information Commissioner. Under certain conditions, by notifying us, you may invoke binding arbitration regarding certain "residual" claims about EU or Swiss Personal Data before a Privacy Shield Panel. Such procedure is in accordance with the rules established under the Privacy Shield. We are subject to the investigatory and enforcement powers of the FTC for EU and Swiss Personal Data.

Links. Our websites provide links (including social media plugins ("Plugins")) that connect to third party websites. Clicking such link establishes a connection and transmits data to/from the operator of such website. Clicking a Plugin while logged in to a social media account may cause the social media website's operator to publish activity to your account. To avoid this, log out of your account before clicking the Plugin link. We are not responsible for and make no representations about the content, security, or privacy practices of any other third party websites. You should read the privacy notices of the websites you visit to understand their data privacy practices.

Changes to Notice. This Notice reflects our business practices. It is not a contract. However, we are required to and will abide by the terms of this Notice as currently in effect. We may amend this Notice at any time. We will notify you of any updates by posting a revised notice on our website. The revised notice will apply to all information collected by us, including previously collected information (for EU or Swiss residents, this applies to the extent permissible under the Privacy Shield). You accept the revised notice by your continued use of our website, products or services following any such amendment. If we revise this Notice in a way that would allow us to disclose your Personal Data to a nonaffiliated third party other than as already described here, we will provide you with a revised notice and give you the opportunity to opt out of any such disclosure. You are responsible to regularly review this Notice. You have the right to a paper copy of this Notice upon request.

Contact. If you have any questions or comments about this Notice or the way that we collect or handle your Personal Data, or if you would like a paper copy of this Notice, please contact our Chief Privacy Officer by any of:

Email: privacy@allianzassistance.com
Phone: 1-800-284-8300
Mail: Allianz Global Assistance
ATTN: Chief Privacy Officer
9950 Mayland Drive
Richmond, VA 23233

Opt Out/Exercise of Rights. To opt out of non-essential marketing communications or non-essential unaffiliated third party information sharing, please contact our Chief Privacy Officer as noted above with your name, policy number. Please include a statement that says "Opt out" (or something similar). Opt outs will be applied to all products and services we provide. We will not unfairly discriminate against any person who chooses to opt out, or exercise any of their rights as described in this Notice.

Electronic Notices. Unless you chose to receive them by US mail at the time of purchase, by purchasing your policy, you consent to receive all notices and documents from us electronically. They will be sent to the email address provided at the time of purchase. You may opt to receive notices and documents from us by mail at any time. If you wish to change or update your notice/documents preferences, email us at customerservice@allianzassistance.com. Please include your name, policy number, and a note that says "Only contact me by mail" (or something similar). You can also let us know by phone at 800-284-8300 or by mail to:

Allianz Global Assistance
ATTN: Customer Service – Only contact me by mail
9950 Mayland Drive
Richmond, VA 23233

If you don't provide an email address at purchase, you'll receive notices and documents by mail. You may request paper copies of any electronic information we send, or update your electronic contact information at any time by emailing or mailing us at the above address, or by calling us. Documents sent to you from us will be in either PDF or HTML format. If you can't receive or read the documents we send you, please contact us so we can assist you.

California Residents. In addition to as defined above, Personal Data may also include information (other than information that is publicly available, de-identified or aggregated), that identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked to a particular California resident or household.

We have collected the following categories of Personal Data from consumers from the sources and for the purposes as described in this Notice in the past 12 months: identifiers, personal information, characteristics of protected classifications, commercial information, biometric information, internet or other electronic network activity information, geolocation data, audio/electronic/visual information, and professional or employment-related information. We use these categories data for purposes as described in Section 1 of this Notice. We do not sell Personal Data. We have disclosed the following categories of Personal Data for business purposes as described in this Notice to the categories of third parties identified in this Notice in the past 12 months: identifiers, personal information, characteristics of protected classifications, commercial information, biometric information, internet or other electronic network activity information, geolocation data, audio/electronic/visual information, and professional or employment-related information.

You may in some cases have certain rights under California law. However, these rights are not available in all cases, and they are subject to applicable exceptions, exemptions, and limitations as provided by law (including without limitation with respect to Personal Data collected pursuant to the Gramm-Leach-Bliley Act). Please contact the Chief Privacy Officer for more information. These rights may include the following: (1) the right to request that we disclose to you the categories and specific pieces of your Personal Data we have collected over the past 12 months; the categories of sources from which that data is collected; the business or commercial purpose for collecting or selling that data; the categories of third parties with whom we share that data; and the specific pieces of that data we have collected about you in that period; the categories of Personal Data sold about you during that period and the categories of third parties to whom that information was sold, by category of Personal Data for each category of third parties to whom the Personal Data was sold; and the categories of Personal Data we disclosed about you for a business purpose during that period; (2) the right to request that we delete Personal Data we have collected about you; (3) the right that we will not discriminate against you for exercising any of these rights, including without limitation by denying goods or services to you; charging a different price or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; providing a different level or quality of goods or services to you; or suggesting that you will receive a different price or rate for, or a different level of quality of, goods or services. You can submit a request to exercise these rights by contacting the Chief Privacy Officer as described above. Upon verification of your request, we will respond to you with the information requested or

confirmation of deletion, or with an explanation for why the information will not be provided or why the data will not be deleted, as applicable.

Effective Date. This Notice was last revised on, and is effective as of, December 31, 2019.