# PRIVACY, SECURITY AND TRANSPARENCY

Our company mission statement requires that we strive to "be a good company," by living up to the trust placed in us by our policyholders, workforce members, vendors and business partners. One of the ways we honor that commitment is by attempting to be transparent about our information collection practices. We extend that same transparency to members of the general public who visit, and use our online and mobile resources. Our privacy statement, contained in the pages that follow, serves, therefore, to give notice about the types of personal information we collect, how we use it, who we share it with and why, and what we do to try to protect it. We delve into those matters in a fair amount of detail in the pages that follow. We encourage you to read them carefully. In the meantime, we provide a quick overview below.

## Summary of how we handle Personal Information

- **What do we collect?**

We collect and retain certain personal information from four different groups of data subjects including our workforce, vendors, customers and visitors to and users of our online and mobile resources. Our privacy statement applies mostly to that last group, from which we collect very little information unless it is voluntarily submitted to us. You can read more about the categories of personal information we collect from that group of data subjects here.

- **Why do we use it?**

We use personal information received from visitors and users of our online and mobile resources to communicate directly with them. Personal information collected from our workforce is used to fulfill our human resources commitments and in furtherance of our legal obligations as an employer, while personal information collected from our policyholder customers is used as needed to carry out the contracts of insurance we have with them. We provide further detail about our use of personal information here.

- **When do we share it?**

We share personal information when needed to our online and mobile resources fulfill our legal obligations and when our vendors and business partners need it to perform under the contracts we have with them. We provide further detail about our sharing of personal information here. We do not sell or rent any personal information to third party data brokers or marketing companies.

- **How do we protect it?**

We maintain a Security Program that is designed to address both technical and operational matters not only within our own company, but also with certain of our vendors and business partners with whom we may share your personal information. Our program also includes an incident response and management and vendor oversight components. You can read about that here and here.

- **Your Privacy Choices and Rights**

You do not have to provide personal information to enjoy most of the features of our online and mobile resources. Moreover, you can opt out of certain activities like newsletters and announcements. You can learn more about that here. Residents of California and data subjects whose personal information was obtained while they were in the GDPR Jurisdictions have certain additional rights. You can read about those here and here.

## Contacting Our Privacy Office

If you have any questions about our privacy and data security policies, procedures and practices, including anything we say in this privacy statement, we encourage you to contact our Privacy Office.


- **Address**
  Attn: Privacy Office
  TMNA Services, LLC
  3 Bala Plaza East, Suite 400
  Bala Cynwyd, Pennsylvania 19004
- **Email:** onlineprivacy@tmnas.com
- **Phone:** 610-227-1300

This privacy statement was amended as of May 22, 2024 and is effective as of that date. The English language version of this privacy statement is the controlling version regardless of any translation you may attempt.

## NAVIGATING THROUGH THIS STATEMENT

You can use the links below to navigate to areas of this statement that apply specifically to you, or which may otherwise be of interest:



## SOME IMPORTANT VOCABULARY

This privacy statement is an important document that explains how we address some of our legal obligations, and your related legal rights, involving personal information. Clarity is, therefore, important. We'll use this section to let you know about some words that have special meanings whenever you see them in this statement. Let's start with the word "**statement**" itself: when we reference "**this statement**", "**this privacy statement**" and "**our statement**", we mean the Privacy, Security and Transparency Statement you are reading now. We use the words "**you**" and "**your**" to mean you, the reader, and other visitors to our online and mobile resources who are, in all cases, over the age of 18. This age requirement is discussed in more detail later in this statement here. We also want to be very clear about exactly what parts of the Tokio Marine corporate enterprise are covered by, and adhere to the policies and procedures explained in this statement.

The Tokio Marine Group ("**TMG**") is a global insurance enterprise with over 200 companies around the world. In the United States, the parent company for approximately 30 of those companies is Tokio Marine North America, Inc. ("**TMNAI**"). The administrative functions (including human resources), for some, though not all, of those U.S.-based companies are centralized and consolidated through a single shared services organization known as TMNA Services, LLC ("**TMNAS**"). So, when we refer to "**Tokio Marine**" or "**we**", "**us**" or "**our**", throughout this statement, we are referring only to TMNAI, TMNAS and those additional companies who have specifically chosen to consolidate their privacy and data security compliance programs though TMNAS. Generally, each of those companies will link directly to this statement. This statement and the rights and obligations it outlines, do not apply to any other affiliated or subsidiary companies of TMG.

When we talk about our "**online and mobile resources**", we mean all websites, portals or other features we operate to allow you to interact with us and our systems, as well as the mobile apps we've created and distributed to let you interact with the content we provide. An "**affinity action**" is when you "follow" us, "like" us or take a similar or analogous action on our external social media presence. As described here, we have a broad array of legal obligations to protect your personal information. So when we use the term "**vendors**" we mean it to include all analogous terms under the data privacy and security laws applicable to us such as "third party service providers" under the New York Department of Financial Services' Cybersecurity Regulation ("**NYCyberReg**") and National Association of Insurance Commissioners' Data Security Model Law ("**NAIC Model Law**"), "processors" and "sub-processors" under the European General Data Protection Regulation ("**GDPR**") and its directly related US-EU Data Privacy Framework, US-Swiss Data Privacy Framework, and U.K. Extension to the EU-US Data Privacy Framework (collectively, the "**Privacy Framework**"), "service providers," "contractors," and "third parties" under the California Consumer Privacy Act ("**CCPA**"), and "service providers" under the Gramm-Leach-Bliley Act ("**GLBA**"). When we say "**business partners**" we mean entities such as the insurance brokers, and certain types of the insurance "producers" and "agents" who offer our products, as all of those terms are defined in the NYCyberReg and NAIC Model Law. When we reference the "**GDPR Jurisdictions**" we mean the countries comprised by the

European Economic Area, the United Kingdom, Switzerland and Japan which, having received an "adequacy decision" from the European Commission, adheres to the material terms of the GDPR.

Finally, and perhaps most importantly, when we refer to "**personal information**", we mean information that can be used to identify or easily be linked to you. The privacy laws in some jurisdictions include unique elements in what they consider to be the personal information of the data subjects they protect. If those laws apply to us, as in the case of the CCPA, then, when the context requires, our use of the phrase "personal information" includes the unique elements required by such laws.

## WHAT PERSONAL INFORMATION DO WE COLLECT?

We collect personal information from four groups of data subjects:

- visitors to, and users of, our online and mobile resources
- current members of our workforce and those who apply for posted jobs
- our third party vendors and business partners
- our policyholders (i.e., our customers) and those who apply directly to us to become policyholders

The categories of information we collect from each of these groups differs. As you may have noticed, it's possible that the same person could fall into more than one group. For instance, someone who is a policyholder might also work for one of our vendors. Or someone who works for us might, on their day off, visit one of our general websites. We explain below the different categories of personal information we collect from each group of data subject.

### Visitors and Users of our Online and Mobile Resources

If you visit and/or use our online and mobile resources, we collect and retain personal information through automated/technical means. We describe that automatic collection here. In addition to that, if you choose to participate in, or make use of certain activities and features available via our online and mobile resources, you will need to provide us with information about yourself. We describe that type of voluntary submission immediately below. ***By using our online and mobile resources, you are signifying to us that you agree with our privacy statement and that we may use and disclose your information as described***.

Voluntarily Submitted Information.
Here are some of the ways you voluntarily give us your personal information. The types of personal information you will be submitting to us in these situations is almost always limited to **identifiers** such as your name, email address, mailing address and phone number. You can read about how we use that personal information here.

- **Emails and Texts –** If you choose to send us an email from our "contact us" link or a similar link, you will be giving us your email address and any other personal information that may be in your message or attached to it. The same is true if you send us a text message.

- **Chatbots Features –** If you interact with a chatbot on our online and mobile resources, you will be giving us, as well as the vendor who provides that service, user chat data, which generates a transcript of your communication with us after our conversation has concluded. By interacting with a chatbot, you may also be providing technical and usage data. Our use of this data is limited to providing information you have requested, processing any transactions you have requested, helping us understand how users interact with our online and mobile resources and to design a better user experience for you.

- **Creating Accounts; Signing up for Newsletters –** If we make an account creation feature available to the general public (that is, to visitors/users who are not our policyholders or workforce members) you will be giving us at least your email address and potentially other identifiers. The same is true if you sign up to receive a newsletter or other informational or marketing material we publish.

- **Registering for Events –** When you register for events, conferences or programs we ourselves may host (rather than outsource to a third party event manager with its own privacy policies), you will be submitting the types of identifiers described above. If the event requires a fee, we may also ask you to submit **credit card or other financial information**.

- **Community Features –** Some of our online and mobile resources may offer social media-like community features letting users post or upload messages, comments, and/or image or other files and materials. If you choose to make use of these features the information you post, including your screen name and any other personal information, will be shared with us and other users of the community features of our online and mobile resources. You understand that we (and you) are not able to control information that you share with other users or make available to third parties through the community features.

- **Customer Portals and Job Applicants –** Some of our online and mobile resources are used to help us serve our policyholders and allow candidates to apply for available jobs. We discuss personal information submitted in those situations elsewhere in this statement such as here and here.

If you prefer we not receive the above-described personal information, please don't submit it. This means you shouldn't participate in the applicable activities on, or use the applicable features available from our online and mobile resources. Such participation and use is strictly your choice. By not participating, you may limit your ability to take full advantage of the online and mobile resources, but most of the content in our online and mobile resources will still be available to you.

Automatically Collected Information.
When you visit or use our online and mobile resources, **basic information about your internet/electronic activity** is automatically collected through your browser via tracking technologies, such as "cookies." Cookies are small text files downloaded onto your computer or mobile device. Cookies allow us to collect your **IP address** and recognize your computer or mobile device and store some information about your preferences for using our online and mobile resources or past actions, such as:

- the type of browser and operating system you use
- the date and time and length of your visit
- the pages visited, graphics viewed and any documents downloaded
- links to other sites you accessed from our online and mobile resources or used to navigate to our online and mobile resources

Additional information about cookies and tracking technologies is available here. If you access our online and mobile resources from a phone or other mobile device, the mobile services provider may transmit to us certain information such as uniquely identifiable mobile device information. That, in turn, allows us to collect **mobile phone numbers and associate them with the mobile device identification information**.

Finally, when you use our online and mobile resources, we may allow third party service providers to place their own cookies or similar technologies in order to engage in the same types of collection we describe above. For example, some Tokio Marine companies covered by this statement use third party "web analytics" services such as those offered by Google Analytics. For more information on how Google specifically uses this data, go to www.google.com/policies/privacy/partners/. You can learn more about how to opt out of Google Analytics by going to https://tools.google.com/dlpage/gaoptout.

User Beware: External Sites, Apps, Links and Social Media.
Some Tokio Marine companies maintain a presence on one or more external social media platforms such as Twitter, Facebook, YouTube and LinkedIn. We may further allow the community features of our online

and mobile resources to connect with, or be viewable from, that external social media presence. Similarly, our online and mobile resources may contain links to other websites or apps controlled by third parties.

We are not responsible for either the content on, or the privacy practices of, social media platforms, or any third party sites or apps to which we link. Those apps, sites and platforms are not controlled by us and therefore have their own privacy policies and terms of use. **To be clear: neither this statement nor the terms of use appearing on or in any of our online and mobile resources apply to our social media presence or any third party sites or apps to which we may link**. That means even if you take an affinity action on our specific social media presence, and identifiers about you are automatically collected and given to us as a result, that collection and transfer is governed by the privacy policies and other terms of the applicable social media platform and are not our responsibility. If you have questions about how those apps, sites and platforms collect and use personal information, you should carefully read their privacy policies and contact them using the information they provide.

**Personal Information we collect from our Policyholders**

Policyholders enter into contracts of insurance with us. Each contract is separate from this statement and has its own terms and conditions for notice of collection and governing our overall confidentiality, data privacy and data security obligations. As a result, those terms, and not this statement, apply to the personal information of policyholders.

For those who apply to become policyholders, we provide notice of what personal information we collect on the proprietary documents that are part of our application process, or the apps and portals we operate for such purpose, doing so via confidential Tokio Marine terms and conditions published thereon. In some cases, policyholder applicant data will be collected by one of our business partners, such as a non-exclusive agent or broker, and shared with us. In those situations, the legal responsibility to provide notice rests with that business partner, not Tokio Marine.

**Personal Information we collect from our Workforce and Job Applicants**

We collect and retain the types of **professional or employment related personal information** you would expect a U.S. employer to have about its U.S. workforce such as name, age, home address, and personal information for payroll, tax and benefits. When the law allows or requires (such as for compliance with equal opportunity/non-discrimination laws) we may also collect **characteristics of protected classifications** such as race, gender, and ethnicity. Similarly, when someone applies for an open job position, including via portals or other online and mobile resources, we collect the personal information we need, and which the law allows, to evaluate their applications.

We provide notice of what personal information we collect from our workforce/applicants in our confidential human resources manuals and other documentation, or on the proprietary apps and portals we operate for such purpose doing so via confidential Tokio Marine terms and conditions published thereon. In some cases, portals and apps may be operated by third parties who transfer the personal information to us. In those situations, the legal responsibility to provide notice usually rests with the third party, not Tokio Marine. You can read about how we use the personal information we collect from our workforce and job applicants here.

**Personal Information we collect from Vendors and Business Partners**

Like all large corporate enterprises, we buy goods and services, lease equipment and office space and attend industry events. In doing so, we interact with many existing and potential vendors and business partners from whom we necessarily collect certain personal information in connection with our contractual and business relationships. Typically, the categories of personal information collected in those cases will be limited to what is often referred to as "**minimum business contact information**" such as name, business title, business address and business email. As a result, if legally required, we make a reasonable effort to provide notice at the point of collection, or address the question of notice in the applicable business contract.

## HOW DO WE USE THE PERSONAL INFORMATION WE COLLECT?

We use personal information we collect only in the manner and through the means allowed by applicable law. That means we determine whether we have a lawful basis/legitimate business purpose to use your personal information before doing so. As stated in applicable law, such lawful bases/legitimate business

purposes include receiving express consent, operating our business, performing a contract, and complying with a legal obligation. More specifically, we use the personal information of each group of data subjects as follows:

### Visitors and Users of our Online and Mobile Resources

We use the automatically collected personal information described here to compile generic reports about popular pages/features of our online and mobile resources, and to see how users are accessing our online and mobile resources and in some cases (such as affinity actions) send materials to you. We use the personal information you voluntarily submitted, as described here, to respond back directly to you and/or send you the information you requested or about which you inquired. We also may use any such personal information you provide to customize our programs and newsletters to make them more relevant to you. We do not sell or rent personal information automatically collected by, or which you voluntarily provide when using our online and mobile resources.

### Our Policyholders

We use personal information collected from our policyholders to administer their policies and process their claims. As mentioned above, policyholders enter into confidential contracts of insurance with us and those contracts have their own terms and conditions describing the manner and means of our use of policyholder personal information. As a result, those terms and not this statement, apply to our use of the personal information of policyholders. We use personal information collected from policyholder applicants to evaluate their applications and underwrite and provide premium quotes. We provide notice of our scope of use via confidential Tokio Marine documents or by publication on the proprietary apps and portals we operate for such purpose.

### Our Workforce and Job Applicants

We use personal information collected from our workforce to operate our business, perform our duties as an employer, and fulfill our commitments to workforce members (such as benefits administration). We use personal information collected from job applicants to evaluate their candidacy and process their applications. We describe our use of workforce and job applicant personal information in greater detail in confidential Tokio Marine human resource policy documents or by publishing such policies on the proprietary workforce/applicant portals and apps we operate.

### Vendors and Business Partners

We use the personal information collected from our vendors and business partners (which, again, is largely minimum business contact information) to manage, administer and perform under our contracts with them, or share information about our products. We also may from time-to-time use personal information about their individual personnel to perform background checks on those who are provided access to our facilities or technology networks so that we can help protect the personal information of others stored thereon. We describe our use of vendor and business partner personal information in greater detail in our confidential contracts with those parties.

## WHEN/WITH WHOM DO WE SHARE PERSONAL INFORMATION?

We may share your personal information as described below. This sharing applies to the personal information of all four groups of data subjects described here.

### Affiliates

We may share personal information to other companies within TMG who will use such information in the same way as we can under this statement.

### Legal Requirements

We may disclose personal information to government authorities, and to other third parties when compelled to do so by such government authorities, or at our discretion or otherwise as required or permitted by law, including responding to court orders and subpoenas.

**To Prevent Harm**

We also may disclose such information when we have reason to believe that someone is causing injury to or interference with our rights or property, or harming or potentially harming other persons or property.

**Business Sale/Purchase**

If TMNAI, TMNAS or any of the companies covered by this statement, or any of their affiliates or subsidiaries, sell or transfer all or substantially all of their assets, equity interests or securities, or are acquired by one or more third parties as a result of an acquisition, merger, sale, reorganization, divestiture, consolidation, or liquidation, personal information may be one of the transferred assets.

**Vendors and Business Partners**

We also share personal information with those of our vendors and business partners who need it to perform under the contracts we have with them. As part of our Security Program, we have adopted standards for those vendors and business partners who receive personal information from us. We attempt to bind such vendors and business partners to those standards via written contracts. Such standards include expectations that when we share personal information with our vendors and business partners, they will comply with all applicable privacy and data security laws and regulations and our Security Program, and will contractually require and cause their subcontractors and agents to do the same. We further attempt to contractually restrict what our vendors and business partners can do with the personal information we provide to them such that it:

- is used only to the minimum extent necessary to carry out the business purpose for which it was provided
- is not disclosed to anyone else without our consent or under our instruction
- remains, as between us and the applicable vendor or business partner, our property
- is not transferred out of the United States without our consent

For any personal information our vendors and business partners process or store at their own locations, we further expect them to use technology infrastructure meeting, at least at the facilities level, minimum recognized standards for security controls. Such recognized standards include those published by the International Standards Organization, the National Institute of Standards and Technology, the AT 101 standards (for data security matters) published by the American Institute of Certified Public Accountants, the Payment Card Industry Security Standards Council, or any reasonably equivalent standards.

***Please note, however, that we cannot guarantee that all of our vendors and business partners will agree to the above-described contractual requirements; nor can we ensure that, even when they do agree, they will always fully comply.***

## YOUR RIGHTS AND OPTIONS

If we are using your personal information to send you marketing materials, such as newsletters or product alerts via text or email, you may opt out by following the opt-out instructions in the email or other communication (e.g., by responding to the text with “STOP” or following the “unsubscribe” link in an email). When we receive your request, we will take reasonable steps to remove your name from our distribution lists, but it may take time to do so. You may still receive materials for a period of time after you opt out. In addition to opting out, you have the ability to access, amend and delete your personal information by contacting us using the contact information below. Opting out of or changing affinity actions or other submissions or requests made on our third party social media platform, will likely require that you do so directly on that platform as we do not control their procedures. Please be aware that if you request us to delete your personal information, you may not be able to continue to use certain features of our online and mobile services. Also, even if you request that we delete your personal information, we may need to retain

certain information for a limited period of time to satisfy our legal, audit and/or dispute resolution requirements.

Some browsers have a "do not track" feature that lets you tell websites that you do not want to have your online activities tracked. At this time, we do not specifically respond to browser "do not track" signals.

## HOW DO WE PROTECT COLLECTED PERSONAL INFORMATION?

### Our Data Security Program

The state licensed insurance companies of Tokio Marine are heavily regulated. In terms of data security and privacy, our various companies are governed by, among other standards, rules, regulations and statutes:

- the Privacy Framework, which flows-down obligations from GDPR and other applicable laws
- the Payment Card Industry Data Security Standards
- the laws adopted by various states using the NAIC Model Law
- the NYCyberReg
- the U.S. federal GLBA
- the CCPA, New York Shield Act and similar state laws

Hopefully we don't need to point out that we take these obligations very seriously. As such, we have adopted, implemented and maintain an enterprise-wide corporate information security and privacy program that includes technical, organizational, administrative, and other security measures designed to protect, as required by applicable law (including all those described above), against reasonably anticipated or actual threats to the security of your personal information (the "**Security Program**"). Our Security Program was created by reference to widely recognized industry standards such as those published by the International Standards Organization, National Institute of Standards and Technology and the Payment Card Industry Security Standards Council. It includes, among many other things, procedures for assessing the need for, and as appropriate, either employing encryption and multi-factor authentication or using equivalent compensating controls. We therefore have every reason to believe our Security Program is reasonable and appropriate for our business and the nature of foreseeable risks to the personal information we collect. We further periodically review and update our Security Program, including as required by applicable law.

### Our Incident Response and Management Plan

Despite the significant investment we've made in, and our commitment to, the Security Program including enforcement of our third party oversight procedures, we cannot guarantee that your personal information, whether during transmission or while stored on our systems, otherwise in our care, or the care of our vendors and business partners, will be free from either failed or successful attempts at unauthorized access or that loss or destruction will never occur. Except for our duty to maintain the Security Program under applicable law, we therefore necessarily disclaim, to the maximum extent the law allows, any other liability for any such theft or loss of, unauthorized access or damage to, or interception of any data or communications including personal information.

All that said, as part of our Security Program, we have specific incident response and management procedures that are activated whenever we become aware that your personal information was likely to have been compromised. Those procedures include mechanisms to provide, when circumstances and/or our legal obligations warrant, notice to all affected data subjects within the timeframes required by law, as well as to give them such other mitigation and protection services (such as the credit monitoring and ID theft insurance) as may be required by applicable law. We further require, as part of our vendor and business partner oversight procedures, that such parties notify us immediately if they have any reason to believe that an incident adversely affecting personal information we provided to them has occurred.

## CHILDREN'S PRIVACY

Federal law imposes special restrictions and obligations on commercial website operators who direct their operations toward, and collect and use information from children under the age of 13. We take those age-related requirements very seriously, and, consistent with them, do not authorize our online and mobile resources to be used by children under the age of 18, and certainly not by anyone under the age of 13. Moreover, we do not knowingly collect personal information from minors under the age of 18.

## THE CALIFORNIA CONSUMER PRIVACY ACT

When we collect personal information from California residents we become subject to, and those residents have rights under, the CCPA, as amended by the California Privacy Rights Act. This section of our statement is used to allow us to fulfill our CCPA obligations and explain your CCPA rights. Our CCPA obligations do not, however, extend equally to all groups of data subjects because we are covered by certain explicit statutory exemptions in the CCPA.

Under those exemptions, the full breadth of CCPA obligations apply to us only with respect to California residents who were visitors to, or users of our online and mobile resources, are part of our workforce or are job applicants, and who communicate with us on behalf of our vendors and business partners. As such, for purposes of this section, the words "**you**" and "**your**" mean only those California residents. For our workforce/job applicants, we have set out our CCPA obligations under a separate notice.

In addition to the definitions set forth at the beginning of this statement, the CCPA contains the following additional definitions:

"**Share**," "**shared**," or "**sharing**" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Information to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

"**Cross-context behavioral advertising**" means the targeting of advertising to a consumer based on that consumer's personal information obtained from activity across businesses or distinctly-branded websites, applications, or services, other than the business or distinctly-branded website, application, or service with which the consumer intentionally interacts. (In other words, if we send you an ad based solely on your interaction with us or our services, this is not cross-context behavioral advertising).

"**Sensitive personal information**" means personal information that is not publicly available and reveals one or more of the following:

- A consumer's Social Security, driver's license, state identification card, or passport number;
- A consumer'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;
- A consumer's precise geolocation;
- A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
- The contents of a consumer's mail, email, and text messages unless we are the intended recipient of the communication;
- A consumer's genetic or biometric data; or
- Personal Information collected and analyzed concerning a consumer's health, sex life, or sexual orientation.

### What did we collect from California Residents?

Certain of the Tokio Marine companies covered by this statement collected from you, within the last 12 months, the categories of personal information already described here. We disclosed this personal information for one or more legal or business purposes as permitted by the CCPA. We urge you to re-read this part of this statement where we describe how we use your personal information and this part where we describe the categories of third parties to whom we may have disclosed it. As stated elsewhere in this statement, we do not sell, and within the last 12 months have not sold, any of your personal information to third parties. We also do not "share" and within the last 12 months have not "shared" any of your personal information to third parties, as the term "share" is defined in the CCPA.

We also may collect "Sensitive Personal Information" which is defined as Personal Information that is not publicly available and reveals one or more of the following:

- Social Security, driver's license, state identification card, or passport number;
- 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;
- racial or ethnic origin, religious or philosophical beliefs, and any other status protected by applicable anti-discrimination laws, or union membership;
- the contents of mail, email, and text messages unless TMNA is the intended recipient of the communication; or
- Personal Information collected and analyzed concerning health, sex life, or sexual orientation.

**Retention of Personal Information**

We retain each category of your personal information for no longer than is reasonably necessary for one or more business purposes, subject to your right to request we delete your personal information. Due to the nature of the services, including the fact that we are subject to various laws and regulations governing the retention of business records, it is not possible to predict the precise length of time that we intend to retain each piece of your personal information. We comply with data retention obligations imposed upon us by law, and those laws, together with best practices in the insurance industry, inform our records retention practices.

When we determine that it is no longer reasonably necessary to retain your personal information for one or more disclosed business purpose(s) based on the above criteria, we will delete your personal information.

**Disclosure of Personal Information**

We may disclose personal information to our "service providers", to our "contractors", and to "third parties" (each as defined by the CCPA) for a business purpose. When we disclose personal information for a business purpose, we enter into an agreement with the receiving party that describes the purpose for sharing the personal information, and that requires the receiving party to keep that personal information confidential. In the case of disclosures to our "service providers," our "service providers" are obligated not to use the personal information for any purpose other than performing the services according to their agreement with us. In the case of our "contractors", our "contractors' are obligated not to use the personal information for any purpose unrelated to the business purpose for which we've engaged them.

**Rights of California Residents**

While we attempt to allow all visitors and users of our online and mobile resources to exercise a degree of control over their personal information, under the CCPA we have a legal obligation to do so for you. More specifically, with respect to your personal information, you have the below-listed rights under the CCPA.

- **Disclosure of Collection/Use** – you have the right to request that we disclose to you, specifically, beyond the general statement immediately above, the categories and specific elements of personal information collected from you including the source of the information and our use of it.

- **Access** – you have the right to receive a copy of the categories and specific elements of personal information we collected about you in the preceding 12 months and/or to request that we transmit your personal information to another entity. To the extent feasible, we will provide and/or transmit your information in a structured, commonly used, machine-readable format.

- **Correct** - you have the right to request that we correct any of your personal information that is inaccurate. We will correct any inaccurate personal information pursuant to your request to the extent possible using commercially reasonable efforts.

- **Disclosure of Sharing** – you have the right to request that we disclose to you, specifically, beyond the general statement immediately above, if your personal information was disclosed or sold to third parties, the categories so disclosed or sold, as well as the categories of third parties who received or purchased it.

- **Delete** – you have the right, under certain circumstances, to request that we delete the personal information we collected about you.

We may deny your deletion request if retaining your personal information is necessary for us or our vendors to:

- Complete the transaction for which we collected your personal information, provide goods or services that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you;
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
- Debug products to identify and repair errors that impair existing intended functionality;
- Exercise free speech, ensure the right of another consumer to exercise their right of free speech, or exercise another right provided for by law;
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.);
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the achievement of such research, if you previously provided informed consent;
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us;
- Comply with a legal obligation; or
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

We may deny your correction request if the personal information is accurate. We may also delete your personal information instead of correcting it to the extent such deletion would not negatively impact you.

Lastly, you have the right to request that we limit the use and disclosure of sensitive personal information by submitting a verifiable request. If you submit such a request, we may continue to use or disclose your sensitive personal information to:

- Complete the transaction for which we collected your personal information, provide goods or services that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you;
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
- Use in a short-term and transient manner, including, but not limited to, to facilitate non-personalized advertising shown as part of your current interaction with our services, but not including disclosure to third parties or use outside your current interaction with our services;
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us; or
- Make any other uses of that information that are permitted by the CCPA and its implementing regulations.

Should you choose to exercise any of your rights under the CCPA, we will not:

- Deny you goods or services;
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties;
- Provide you a different level or quality of goods or services; or
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

However, please be aware that it may be a functional necessity for our online and mobile services to have personal information about you in order to operate, and we may not be able to provide some or all of our online or mobile services to you if you direct us to delete your personal information.

You can exercise these rights up to two different times every 12 months. To do so, just contact us at datarights@tmnas.com or **1-855-218-6627**. We may ask you to fill out a request form. The CCPA only allows us to act on your request if we can verify your identity or your authority to make the request, so you will also need to follow our instructions for identity verification. After we receive your request, we will provide to you, in writing and free of charge (unless your request is excessive, repetitive, or manifestly unfounded),

the requested information for the 12-month period preceding your request (unless you specifically request disclosure beyond such 12-month period, in which case, we will process your request with respect to personal information we have collected during the time period you specify, provided that (a) the earliest date that your request may apply to is January 1, 2022, and (b) processing your request does not require disproportionate effort). You can choose to have this information delivered to you by postal mail or electronically. We will try to respond to your verified request within forty-five (45) days of receipt, but if we require more time (up to another forty-five (45) days) we will inform you of the reason and extension period in writing. Please note that we are not required to comply with your request for information more than twice each year. If applicable, our response will explain the reasons why we cannot comply with your request.

If you make a verifiable request per the above, we will confirm our receipt and respond in the time frames prescribed by the CCPA.

## DATA PRIVACY FRAMEWORK AND PERSONAL INFORMATION FROM OUTSIDE THE US

The Data Privacy Framework administered by the US Department of Commerce and their European Economic Area ("EEA"), Swiss, and United Kingdom (the "UK") counterparts govern the transfer to the United States and subsequent use, retention and further transfer of personal information collected from data subjects located in the GDPR Jurisdictions.

Insurance industry-specific laws in the United States prohibit us from offering our insurance products to those jurisdictions, or anywhere outside the United States. As a result, we cannot, and do not, collect personal information from non-US policyholders or prospective policyholders abroad. Similarly, we do not target or tailor our online and mobile resources or any of our other US-based business activities to appeal to, or specifically attempt to do business in the GDPR Jurisdictions.

Nonetheless, being part of the global TMG enterprise, we do, from time to time, receive intra-company transfers of personal information collected from data subjects in the GDPR Jurisdiction. Specifically, because portions of the TMG global human resources function and related compensation and benefits programs are administered from within the United States, we receive personal information from TMG workforce members around the world, including from the GDPR Jurisdictions. Those transfers are undertaken in accordance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (collectively, the "**Data Privacy Framework**").

TMNAS, First Insurance Company of Hawaii, Ltd., Maguire Insurance Agency, Inc., and Tokio Marine Management, Inc., who have specifically chosen to consolidate their privacy and data security compliance programs though TMNAS, comply with the Data Privacy Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the EEA, Switzerland, and the UK to the United States. TMNAS has certified to the U.S. Department of Commerce that these entities adhere to the Data Privacy Framework Principles. If there is any conflict between the terms in this privacy statement and the Data Privacy Framework Principles, the Data Privacy Framework Principles shall govern. To learn more about the Data Privacy Framework program, and to view our certification, please visit https://www.dataprivacyframework.gov.

The Data Privacy Framework is predicated on the seven core principles listed below. You can read the Department of Commerce's official description of those principles here. You can read about how we specifically comply with them below.

- **Notice** – We provide notice of collection to US-based data subjects as described in this statement. As already discussed, we do not ourselves collect personal information from data subjects in the GDPR Jurisdictions. When a TMG company engages in such collection it complies with the notice requirements of Articles 13 and 14 of the GDPR or the applicable provisions of equivalent data protection laws of the GDPR Jurisdictions (the "**TMG GDPR Notice**").

- **Choice** – The choices we make available to US-based data subjects to limit the use and disclosure of their personal information are described in this statement. The choices available to data subjects from the GDPR Jurisdictions to limit the use and disclosure of their personal information are set forth in Articles 18 and 21 of the GDPR or the applicable provisions of equivalent data protection laws of the GDPR Jurisdictions.

The TMG company engaged in the original collection of personal information flows those choice obligations down to us and we fully comply with them. These rights may include certain limits on the use or disclosure of personal information to a third party, other than to a third party acting as an our agent to perform tasks on our behalf and under our instructions. With respect to sensitive information, we will obtain your affirmative express consent if such information is to be disclosed to a third party or used for a purpose other than that for which it was originally collected or subsequently authorized by you. If you have any questions or if you wish to exercise your right to limit the use and/or disclosure of your information, you may contact us at **onlineprivacy@tmnas.com** or at the address at the end of this statement.

- **Accountability for Onward Transfer** – Information about our accountability under the Data Privacy Framework is found here. We adhere to this principle via our third party oversight procedures. As is the case with U.S. state and federal law in general, we remain responsible under the Data Privacy Framework principles if third parties we engage to process your personal information do so in a manner inconsistent with the principles, unless we can prove that we are not responsible for the event giving rise to any harm you may incur.

- **Security** – We adhere to this principle through our Security Program and our third party oversight procedures.

- **Data Integrity and Purpose Limitation** – We describe the uses we make of personal information collected from US-based data subject elsewhere in this statement. Personal information transferred to us under the Data Privacy Framework is used only in a manner consistent with the original TMG GDPR Notice provided to the data subject.

- **Access** – For US-based data subjects, we provide access to collected personal information as required by law such as described here. The rights of access available to data subjects from the GDPR Jurisdictions are set forth in Articles 15, 16, 17 and 20 of the GDPR or the applicable provisions of equivalent data protection laws of the GDPR Jurisdictions. The TMG company engaged in the original collection of personal information flows those access obligations down to us and we fully comply with them, through that TMG company. These rights include the right to access your personal information and, subject to certain limitations, may also include the right to correct, amend or delete your personal information if it is inaccurate or was collected in violation of these Principles. If you have any questions or if you wish to exercise your right to access your information, you may contact us at **onlineprivacy@tmnas.com** or at the address at the end of this statement.

- **Recourse, Enforcement and Liability** – Our overall Security Program includes processes and procedures to annually verify our compliance with this Data Privacy Framework section of our statement. If individuals believe that we are not compliant, or if they have other complaints related to this Data Privacy Framework section of our statement or our conduct under it, we encourage those individuals to contact us using the contact information listed at the end of this statement. We commit to investigate and attempt to remedy all valid complaints.

The United States Federal Trade Commission or "**FTC**" has jurisdiction over our compliance with the Data Privacy Framework and we are subject to the FTC's investigatory and enforcement powers. Our adherence to the Data Privacy Framework may be limited to the extent required to satisfy legal obligations including national security or law enforcement requirements. If there is any conflict between the policies in this privacy statement and the Data Privacy Framework principles, the Data Privacy Framework principles shall govern with respect to personal information collected from data subjects in the GDPR Jurisdictions.

Inquiries or complaints regarding our Data Privacy Framework compliance can be directed to us at the email or physical address / phone number found here. **Directing such inquiry/complaint to the specific attention of "Data Privacy Framework Inquiries and Complaints" will facilitate a more prompt response.**

Unresolved complaints under the Data Privacy Framework will be referred to the BBB National Programs, a non-profit alternative dispute resolution provider located in the United States and operated by the Council of Better Business Bureaus. The BBB is authorized to provide dispute resolution services under the Data Privacy Framework. If you do not receive timely acknowledgment of your complaint from us, or if your complaint is not satisfactorily addressed, please visit https://bbbprograms.org/programs/all-programs/dpf-consumers/ProcessForConsumers for more information and to file a complaint. If your complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available before a Data Privacy Framework Panel for European Union individuals. For disputes involving human resources data, TMNAS cooperates and complies with the EU Data Protection Authorities, the Swiss Federal Data Protection and Information Commissioner, and/or the UK Information Commissioner's Office.

## CHANGES TO THIS PRIVACY STATEMENT

We may modify or update this statement periodically with or without prior notice by posting the updated policy on this page. You can always check the "Last Updated" date at the top of this document to see when the statement was last changed. If we make any material changes to this statement, we will notify you by reasonable means, which may be by e-mail or posting a notice of the changes on our website or through our mobile app prior to the changes becoming effective. We encourage you to check this statement from time to time. IF YOU DO NOT AGREE TO CHANGES TO THIS STATEMENT, YOU MUST STOP USING OUR ONLINE AND MOBILE RESOURCES AFTER THE EFFECTIVE DATE OF SUCH CHANGES (WHICH IS THE "LAST UPDATED" DATE OF THIS STATEMENT).

## CONTACTING US

If you have questions about our privacy statement or privacy practices, please contact our Privacy Office:

**Attn: Privacy Office**
**TMNA Services, LLC**
**3 Bala Plaza East, Suite 400**
**Bala Cynwyd, Pennsylvania 19004**
**610-227-1300**
**onlineprivacy@tmnas.com**