PRIVACY AND TRANSPARENCY AT TOKIO MARINE

Tokio Marine honors its trusted relationships with consumers, employees and the partners with whom we work by offering transparency into the manner in which we collect data and the ways in which we potentially share it with others. We encourage you to explore this page and the pages and policies to which it links in order to better understand where and how we may be collecting your data and what we do with it.

You should note that we centralize and consolidate the administrative functions of our U.S.-based businesses, including human resources, through a single shared services organization known as TMNA Services, LLC. Consequently, when we refer to "Tokio Marine", "TMNAS", "we", "us" or "our", throughout this page and the pages and policies to which it links, we are referring to TMNA Services, LLC, as well as each of the U.S.-based insurance businesses that we have designated as being covered by these policies by listing them here.

If you have any questions about our privacy policies or practices, we encourage you to contact our Privacy Office. We provide the information by which you can do so below.

Information Collected

- **Online**

We collect, retain and use certain information from visitors to the Internet-based resources we make available such as our corporate web sites www.tmnas.com and our unbranded sites, sites for our products and services.

Our Online Privacy Policy describes the types of information we collect online, the passive and active ways we collect it and the circumstances under which we may share it. You can read our Online Privacy Policy here.

- **Commerce**

We do all of the things you would expect from a large company such as buy goods and services, lease equipment and office space and attend industry events. In doing so, we interact with many existing and potential suppliers, customers and business partners from whom we necessarily collect certain information to manage, administer and perform under contracts, or share information about our products.

The programs and procedures we use to ensure privacy in our general business are described here.

- **Workplace**

We collect, retain and use certain information about prospective, current, and in some cases former, members of our workforce to fulfill our human resources commitments and in furtherance of our legal obligations as an employer.

Our Human Resource Privacy Policy has the details here.

- **Privacy Shield Compliance**

We conduct business, among other places, in Switzerland and many of the countries comprising the European Economic Area. Since our commitment to transparency and trust in matters of privacy does not end at the US border, for information transferred from those countries to our United States operations, we comply with the US-EU Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the U.S. Department of Commerce. Our Privacy Shield Policy can be read here. You can verify our good standing under the Privacy Shield by searching our name here.

Contacting 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

ONLINE PRIVACY POLICY HIGHLIGHTS

This page highlights some of the key elements of our Online Privacy Policy. Both this page and our Online Privacy Policy apply to www.tmnas.com, the official web site of Tokio Marine, the site we publish for our various products and services and any authorized online apps or features that may contain a link to this policy. For more information, please read our complete Online Privacy Policy.

Information Collected

There are two types of information that we obtain from you online, and then store and use:

- non-personal information that's collected automatically; and
- personal information that you voluntarily provide to us

We do not collect any personal information from you when you visit our site unless you expressly and voluntarily participate in an activity that asks for it and you voluntarily provide it. To put it another way, FOR US TO HAVE ACCESS TO YOUR PERSONAL INFORMATION, YOU HAVE TO HAVE MADE A CHOICE TO KNOWINGLY GIVE IT TO US.

More details

Uses of Information

We use voluntarily provided personal information to communicate directly with you including via email, postal mail, and phone. We do not sell or rent your personal information to third party data vendors or marketing companies. As you might expect, we also disclose your information when required by law.

We use non-personal information to administer our site, make it better, and to make business decisions about what programs our customers might like.

More details

Your Privacy Choices

You do not have to provide personal information to enjoy most of the features of our site. You also can opt out of certain activities like newsletters and announcements by sending us an opt-out email.

More details

Privacy Shield Compliance

We comply with the US-EU Privacy Shield Framework and the Swiss-US Privacy Shield Framework established by the US Department of Commerce regarding the collection, use, and retention of certain personal information from European Economic Area member countries and Switzerland. We will collect, use and retain such information in accordance with our Privacy Shield standards.

More details

Contacting Us

Questions about this highlights page or our Online Privacy Policy may be sent to:

Attn: Privacy Office
TMNA Services, LLC
3 Bala Plaza East, Suite 400
Bala Cynwyd, Pennsylvania 19004

You may also reach us by phone:

610-227-1300

Or by email: **onlineprivacy@tmnas.com**

ONLINE PRIVACY POLICY

Thank you for visiting Tokio Marine's online resources and viewing this privacy policy. We use this policy to tell you about the types of information we collect from you when you visit our site or use authorized features or apps that link to this policy. More specifically, this policy tells you:

- the types of information we collect when you visit our website and how we collect it;
- the ways in which we use, share and protect that information;
- the choices you have in controlling the collection of your information; and
- your ability to access and update your information.

By using our sites or other online resources, you are signifying to us that you agree with this policy. Although the site and resources may contain links to other websites controlled by third parties, you should be aware that we are not responsible for the privacy practices of those, or any other, sites. If you have questions about how those websites collect and use data, you should carefully read those sites' privacy policies.

This privacy policy was amended on April 20, 2017 and is effective as of that date.

Some Important Vocabulary

This privacy policy is a legal document, so clarity is important. We'll use this section to let you know about some words that have special meanings whenever you see them in this policy. Let's start with the word "policy" itself: when we reference "this policy", "this privacy policy" and "our policy", we mean the Tokio Marine Online Privacy Policy you are reading now. We use the words "you" and "your" to mean you, the reader, and other visitors to our site who are, in all cases, over the age of 18. This age requirement is discussed in more detail later in this policy here.

Whenever we reference "this site", "our site" or "the site", we mean the Tokio Marine web site(s) found at www.tmnas.com and such others as we may make available from time to time. When we talk about "authorized features and apps", we're referring both to elements of our social media presence viewable from Facebook, Twitter, YouTube, Google+, LinkedIn or any of the many other available external third party social media platforms, as well as mobile or other apps we've created and distributed to let our customers and followers view our site or otherwise interact with our content. Last, but definitely not least, when we refer to "personal information", we mean information that can be used to identify you or that can be easily linked to you. Thus, a fairly comprehensive list of "personal information" would include such things as your name, address, telephone number, fax number, email address, social security number and date of birth. In contrast, a domain name or an internet protocol address, would not be considered personal information.

Privacy Shield Statement

Consistent with our goal of trying our best to keep your information secure, we comply with the US-EU Privacy Shield Framework and the Swiss-US Privacy Shield Framework established by the US Department of Commerce (collectively, the "**Privacy Shield**"). The Privacy Shield governs the collection, use, and retention of personal information from the countries comprising the European Economic Area and Switzerland. As part of our certification, we've implemented and maintain a set of privacy standards that are approved by the United States, the European Economic Area and Switzerland. Those privacy standards are discussed in more detail later in this policy here.

Please be a Grown Up: User Age Requirements and 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 intend for this site or any of our authorized features or apps 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. If we become aware that anyone under the age of 18 has submitted personal information to our site, we will delete that information and will not use it for any purpose whatsoever. We encourage parents and legal guardians to talk with their children about the potential risks of providing personal information over the Internet.

Nothing Personal: Automatically Collected Information
When you visit our site, basic information is passively collected through your browser via use of tracking technologies, such as "cookies" which utilize various files sent from our servers to your computer hard drive. Additional information about cookies and tracking technologies is available here. The information we collect through cookies and other means is **not personal information** and does not individually identify you. It includes things like:

- the domain name and IP address from which you accessed our site
- the type of browser and operating system you use
- the date and time and length of your visit
- the specific page visited, graphics viewed and any documents downloaded
- the specific links to other sites you accessed from our site
- the specific links from other sites you used to access our site

Mobile devices are the one possible exception to the rule that our passive, automatic collection activities exclude personal information. We say that because, if you access our site from a phone or other mobile device, the mobile services provider may transmit to us uniquely identifiable mobile device information which allows us to then collect mobile phone numbers and associate them with the mobile device identification information. Some mobile phone service providers also operate systems that pinpoint the physical location of devices and we may receive this information as well.

Regardless, we use both automatically collected non-personal information and mobile device information only to compile generic reports about popular pages on our site, and to see how our customers and followers are accessing our site. We then use that data to administer the site, make your activities more convenient and efficient and to enhance the functionality of our site, such as by remembering certain of your information thereby saving you time.

Now its Personal: Voluntarily Submitted Information
If you participate in certain activities on our site, you may need to provide us with information about yourself such as your name, email address, mailing address, phone number, or fax number. For example, if you choose to send us an email or fill out an online form, you are voluntarily providing personal information to us. In doing so, you are giving us your consent to collect, use and disclose that information for the purpose it is requested and for other reasonable internal business purposes. We do not sell, rent or trade voluntarily submitted personal information with third parties.

If you don't want us to collect this type of personal information, don't provide it! This means you shouldn't participate in the activities on our sites that request or require it. Participation is strictly your choice. Not participating may limit your ability to take full advantage of the site, but it will not affect your ability to access certain information available on the site to the general public.

Here are some of the ways you voluntarily give us your personal information and how we use it:

- **Emails and Texts -** When you send us an email, your email address and any other personal information that may be in the content of your message or attached to it, are retained by us and used to respond back directly to you. The same is true if you send us a text message. If you prefer we not collect, use or store this information, please do not email or text us. Instead, you may want to communicate with us by phone or by regular mail.

- **Registering for Programs and Our Newsletter -** When you register for programs and our various newsletters, you submit personal information to us which we then retain. We use that information to send you information about the applicable program. We also may use any personal information you provide to customize our programs and newsletter to make them more relevant to you. If you include your email address or a phone number in your registration information we may use it to communicate with you via email and/or phone.

Note that some authorized features and apps may allow users to post or upload messages, comments, screen names, computer files and other materials. If you choose to make personally identifiable information public through these means, we will consider that information to be in the public domain and will not limit its disclosure in the manner described by this policy.

Choices you can make: Opt Out and Account Changes
If we are using personal information you provided to us in order to enable us to send you materials, such as newsletters or product alerts via text or email, and you decide you don't want to receive such materials, you may opt out by following the opt-out instructions in the email or other communication, or the opt-out details provided to you through the applicable program. In addition, you can always opt out by accessing our centralized opt-out link located on our site in order to opt out of any programs in which you may be enrolled. When we receive your request, we will take reasonable steps to remove your name from our distribution lists. Users also need to understand it may take a period of time to remove your name from our lists after your request and due to such latency 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. To learn more about your Access rights under the Privacy Shield, click here.

Things Happen: We do what we can to ensure your privacy
We will take all reasonable security precautions to protect your personal information provided to our site. Due to the inherently open and somewhat risky nature of the Internet, however, we cannot guarantee that your information, whether during transmission or while stored on our systems or otherwise in our care, will be free from unauthorized access or that loss, misuse, destruction or alteration will not occur. We disclaim any liability for any theft or loss of, unauthorized access or damage to or interception of any data or communications. You should also note that third party companies we engage to provide us with services either to help us in our business, or to perform functions we would otherwise perform ourselves will have incidental access to your information, including your personal information, as part of the work they perform. We require that they enter into confidentiality and other agreements, but cannot guarantee their compliance.

Changes to this Privacy Policy
We reserve the right to change or update this policy from time to time. Please check our site periodically for such changes since all information collected is subject to the policy in place at that time. Typically, we will indicate the effective/amendment date at the beginning of this policy. If we feel it is appropriate, or if the law requires, we'll also provide a summary of changes we've made near the end of the new policy.

Contacting Us
If you have questions about our privacy policy 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

COMMERCIAL PRIVACY, CONFIDENTIALITY AND DATA SECURITY POLICY

We use this policy to establish the commitments we make to our suppliers, contractors, consultants and other external business partners with respect to the confidential and personal information we may collect from them in the course of our commercial dealings. We also use this policy to set the minimum standards we require from those same parties so that they know our expectations and so our customers will have some transparency into the policies and procedures we use to try to ensure that the data we store, transmit and process through third parties is protected. More specifically, this policy tells you:

- the quality of the data centers, networks and other physical facilities and technical infrastructure our business partners are expected to use when handling the data we may provide to them

- the standards of confidentiality and data security we expect those partners to apply not only to Tokio Marine's own data, but the data of our employees, customers, and the like

- the standards of confidentiality and data security we apply to personal information we receive from our external business partners and to which we expect them to adhere with regard to information they receive from us

This policy does not supersede the more comprehensive, and typically more stringent terms of the contracts we enter into with our business partners, nor does it alter or replace other policies, notices or consents required by or provided under local law.

This policy is effective as of September 23, 2016 and has not been amended since that date.

General Confidentiality

We engage certain business partners to provide us with services in support of our business including information technology, finance and administrative services. Such services will sometimes involve the storage, handling, transmission or processing of confidential and personally identifiable information. Other business partners may also gain incidental access to data as part of the services they provide including while visiting our facilities.

For our part, we collect information about our business partners and their individual personnel—to perform, for example, background checks on those provided access to our facilities or computer networks. The specific types of information we collect and the ways in which we use it vary with the nature of our contractual relationship. Moreover, the local laws of the location at which our business partners' personnel perform their services often impacts whether and how we collect such information and what we do with it. Some jurisdictions, for instance, require that suppliers' personnel provide prior consent before their information can be collected or used.

In order to continue doing our best to comply with these and similar laws we have, with respect to all confidential, non-public information that may be obtained by any party in the course of our commercial relationships, adopted a comprehensive set of standards to which we expect our business partners to join us in adhering. These standards include expectations that such information will:

- be used only to the minimum extent necessary to carry out the business or services for which it was provided or collected

- not be used or disclosed to anyone without the consent of the disclosing party except to those who have a need to know and are bound by confidentiality and data security obligations consistent with these expectations

- remain the property of the originally disclosing party

- be saved for legal requirements including any archival requirements, be returned to the originally disclosing party or be destroyed/deleted in a manner that makes it non-readable and non-retrievable

Under certain circumstances our business partners and their personnel will require access to Tokio Marine's computer networks and related systems. In such circumstances, we will provide login credentials or other access codes. We expect that our business partners will:

- inform us of the names of the personnel authorized to use such access codes

- notify us immediately if such personnel are terminated or reassigned

- use the access codes only for the purposes for which they are provided and accessing only the specific portions of our system required for their services

- connect to our systems only as directed by us, through our security gateways and/or firewalls

- ensure that all of their individual personnel comply with the foregoing as applicable

Privacy and Data Security

Certain types and elements of confidential and personally identifiable information are subject to special privacy laws or regulations such as the US Gramm-Leach-Bliley Act, the US Health Insurance Portability and Accountability Act and the European Union's Directive on Data Protection.

Our expectation is that when our business partners have any type of access, possession or control of such specially regulated information that they will:

- comply with all applicable privacy and data security laws and regulations including by implementing and maintaining such administrative, technical and physical security procedures, safeguards and practices as may be necessary

- not use such information for any purpose other than for the purpose for which it was given and for our sole benefit

- not transfer such information out of the jurisdiction from which it was obtained without our prior written consent

- shred, destroy or modify any unencrypted information contained in print or electronic media so that it is unreadable prior to disposal

- notify us immediately if they have any reason to believe that there has been an incident (e.g., unauthorized access or use, personnel violating this policy) relating to or affecting such regulated information

- cooperate, at their own expense, with any investigation resulting from such incident and take any action needed to comply with privacy and data security laws and regulations as regards security incidents

- reimburse us for costs incurred in connection with such incidents as well as provide various remedies to any of our affected personnel or customers such as credit monitoring services, identity theft insurance and the like

- contractually require and cause its subcontractors and agents to comply with the foregoing

Where our business partners possess or have access to specially regulated information of ours (to include our customers) we expect to undertake periodic reviews of their policies, procedures and practices used to maintain the privacy, security and confidentiality of the regulated and personal information and/or to allow third parties to conduct such reviews or more formal audits under recognized standards (such as those described below).

Data Center and Network Infrastructure Standards

To the extent a Tokio Marine business partner stores, processes or transmits any Tokio Marine data, we expect that such partners will comply with applicable law with regards to such data and will use data center facilities which in all cases meet, at least at the facilities level, minimum recognized standards for internal controls, security, infrastructure and operations. Such recognized standards include the following or their equivalents:

- the 2700x series standards for security promulgated by the International Standards Organization and International Electrotechnical Commission

- the SSAE 16 standard promulgated by the American Institute of Certified Public Accountants

- the AT 101 standards promulgated by the American Institute of Certified Public Accountants

- the TIA-942/Tier III classification promulgated by the Uptime Institute and the Telecommunications Industry Association (and any successor thereto)

Consistent with these standards, our expectation is that any facility in which Tokio Marine data (to include the data of our employees and customers) is stored will have, at least, dual-factor access control at principal facility access points, on-site security, CCTV surveillance of interior and exterior strategic

locations and access points with retention of video records. We also expect our partners to disclose their facilities and data center locations to us and to tell us in advance if they're going to be changed.

Changes to this Policy

We reserve the right to change or update this policy from time to time. Please check our site periodically for such changes since all information collected is subject to the policy in place at that time. Typically, we will indicate the effective/amendment date at the beginning of this policy. If we feel it is appropriate, or if the law requires, we'll also provide a summary of changes we've made near the end of the new policy.

Contacting Us

If you have questions about our privacy policy 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

PRIVACY SHIELD STATEMENT

This Privacy Shield Statement sets forth the privacy principles TMNAS follows in connection with the transfer and protection of personal information from the European Economic Area ("**EEA**") and Switzerland to the United States. The US-EU Privacy Shield Framework and the Swiss-US Privacy Shield Framework were developed to provide US organizations with a means of satisfying the requirements under the EU Directive on data protection and Article 6 of the Swiss Federal Act on Data Protection respectively.

Consistent with TMNAS's goal to protect personal privacy, TMNAS is fully committed to complying with the US-EU Privacy Shield Framework and Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information transferred from EEA member nations and Switzerland to the United States. TMNAS has certified to the Department of Commerce that it adheres to both the US-EU and Swiss-US Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access and Recourse, Enforcement and Liability as set forth below (the "**Principles**"). The United States Federal Trade Commission (FTC) has jurisdiction over our compliance with the Privacy Shield and we are subject to the FTC's investigatory and enforcement powers. Information regarding the Privacy Shield program and evidence of our certification can be found by visiting https://www.privacyshield.gov/.

This Privacy Shield Statement is effective as of April 20, 2017 and has not been amended since that date.

Scope

This Privacy Shield Statement governs all personal information received by TMNAS in the United States, and its subsidiaries Maguire Insurance Agency, Inc., First Insurance Company of Hawaii, Ltd., and Tokio Marine Management, Inc., from TMNAS's operations and business partners in the EEA and Switzerland. This includes human resources data, and personal data other than human resources data including vendor management data, data from visitors to our websites and personal information from policy holders. TMNAS uses voluntarily provided personal information to: (i) communicate directly with website visitors; (ii) administer their policies and process claims on behalf of policy holders in addition to transferring it to third parties who do the same on our behalf; and (iii) carry out our obligations under employment and benefit laws. TMNAS discloses personal information to our vendors including those with cloud-based software licensed in support of our operations. As used in this Privacy Shield Statement, "personal information" has the meaning given to it under the applicable local law of the country from which it was originally collected. Generally, it means information that identifies or can directly or indirectly lead to the identification of an individual, including such things as an individual's name, address, telephone number, fax number, email address, social security number and date of birth.

Privacy Shield Principles

The Privacy Shield is predicated on seven core Principles:

- **Notice**
- **Choice**
- **Accountability for Onward Transfer**
- **Security**
- **Data Integrity and Purpose Limitation**
- **Access**
- **Recourse, Enforcement and Liability**

We adhere to and have implemented policies and procedures regarding these core Principles in the following ways:

Notice. When we collect personal information from individuals in the EEA or Switzerland, we tell them about the types of personal data or personal information being collected, the purposes of our collection and the nature of our intended uses. We also advise them of the types of third parties to whom we further disclose such information,

the purposes for which we disclose to such third parties, and the choices and means, if any, we offer for limiting use and disclosure as well as how to contact us with inquiries or complaints. We use a variety of different, context-specific means to provide such notice.

Choice. We will offer those individuals whose personal information we've collected a choice. They may "opt out" of having their personal information disclosed to third parties and/or used for purposes other than for the purposes for which it was originally collected or subsequently authorized. For the types of personal information that the laws of the EU countries or Switzerland deem "sensitive" (including ideological views or activities, information on social security measures, or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings under the Swiss-US Privacy Shield Framework), rather than having to opt out after the fact, we afford affected individuals, at the time of collection, an opportunity to "opt in" and specifically consent to have their information disclosed to third parties or used for purposes other than those for which it was originally collected or subsequently authorized. Just as we do in fulfilling our Notice obligations, we use a variety of different, context-specific means to provide the choices described here or otherwise required by the Privacy Shield.

Accountability for Onward Transfer

Our accountability under the Privacy Shield found at https://www.privacyshield.gov/article?id=3-ACCOUNTABILITY-FOR-ONWARD-TRANSFER, for the personal information we receive and subsequently transfer to third parties is described in the Privacy Shield Principles. In summary, we remain responsible and liable under the Privacy Shield Principles if third-party agents that we engage to process your personal information on our behalf 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

At a minimum, we take reasonable precautions to protect the personal information in our possession from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. Please read here for more detail about the standards and expectations we set regarding physical and technical security for personal information.

Data Integrity and Purpose Limitation

We only use the personal information we collect in ways that are consistent with the purposes for which it was originally collected or for which we subsequently obtained authorization from the affected individuals. We take reasonable steps to ensure that the information is reliable for its intended use, accurate, complete, and current. To accomplish this, we necessarily rely on individual data subjects to exercise their access rights to keep us apprised of any changes in their personal information.

Access

If an individual from whom we've collected data writes to us and asks to have access to their personal information, we will take all reasonable steps to ensure such access is granted. Obviously, the relevant information must be in our possession or under our reasonable control for us to do so. Once such access is granted, affected individuals have the right under the Privacy Shield to have us correct, amend or delete their information where it is determined to be factually inaccurate. There are however, certain limitations to an individual's rights to such access. These include situations where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy, or where the rights of persons other than the individual would be violated.

Recourse, Enforcement and Liability

We implement processes and procedures to verify our compliance with this Privacy Shield Statement. If individuals believe that we are not compliant, or if they have other complaints related to this Privacy Shield Statement or our conduct under it, we

encourage those individuals to contact us using the contact information listed at the end of this Privacy Shield Statement. We commit to investigate and attempt to remedy all such valid complaints.

Dispute Resolution
In compliance with the EU-US and Swiss-US Privacy Shield Principles, TMNAS commits to resolve complaints about your privacy and our collection or use of your personal information. European Union or Swiss individuals with inquiries or complaints regarding this privacy policy should first contact TMNAS at:

Edward Sayago, Managing Corporate Counsel
3 Bala Plaza East, Suite 400
Bala Cynwyd, PA 19004
onlineprivacy@tmnas.com
610-227-1300

TMNAS has further committed to refer unresolved privacy complaints under the EU-US and Swiss-US Privacy Shield Principles to BBB EU PRIVACY SHIELD, a non-profit alternative dispute resolution provider located in the United States and operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers/ for more information and to file a complaint.

Please note that if your complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel for European Union individuals.

Additionally, for disputes involving human resources data, TMNAS cooperates and complies with the EU Data Protection Authorities and/or the Swiss Federal Data Protection and Information Commissioner, as applicable, with respect to such data.

Limitation of Principles
Adherence to this Privacy Shield Statement may be limited to the extent required to satisfy legal obligations (including, but not limited to, subpoenas and court orders) and/or meet national security, law enforcement or public interest requirements. We may be required, under certain circumstances, to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. The law also provides certain express exceptions and variations to our obligations under this Privacy Shield Statement.

Online Privacy Policy
We use a separate Online Privacy Policy to inform you about how we collect and use information from visitors to our internet sites and social media presence. Conflicts between the Online Privacy Policy and the Privacy Shield program with respect to personal information received by Tokio Marine in the United States from the EEA or from Switzerland will be resolved in favor of the Privacy Shield Principles.

Changes to this Privacy Shield Statement
We reserve the right to change or update this policy from time to time. Please check our site periodically for such changes since all information collected is subject to the policy in place at that time. Typically, we will indicate the effective/amendment date at the beginning of this policy. If we feel it is appropriate, or if the law requires, we'll also provide a summary of changes we've made near the end of new policy.

Contacting Us
If you have questions about this Privacy Shield Statement, our privacy practices, or would like to submit a complaint, 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

HUMAN RESOURCES PRIVACY POLICY

We use this policy to describe the manner and means we use to protect the information we collect from prospective, current, and in some cases former, members of our workforce. This policy does not create a contract of employment between you and Tokio Marine nor does it modify any contracts of employment or human resources policies, notices or consents we may maintain or obtain within a particular jurisdiction. This policy does not apply to information collected from or received by us outside of any actual or prospective employment relationship. That information, even if it involves individuals who are our employees, is subject to our separate policies described here.

This policy is effective as of April 20, 2017 and has not been amended since that date.

Our Global HR Function

Our global human resources function and related compensation and benefits programs are administered principally from within the United States. For personal information obtained from US-based employees, we comply with all applicable federal and state laws and regulations. If a certain US-based law or regulation requires special protections for sensitive information, we have additional policies and processes in place in order to comply with those requirements. We describe those processes and publish those policies in confidential company documents made available to all affected employees.

With respect to employees based and resident in Switzerland and the EU, the centralized, US-based nature of our HR function means that we necessarily transfer their human resources-related personal information from the European Union and Switzerland to the United States (collectively "**EU HR Data**"). We do so in order for our US-based HR employees and the external business partners who support them to perform HR-services for the benefit of such Swiss and EU-based personnel.

The Privacy Shield

We handle all EU HR Data with at least the same degree of care as that of our US-based employees. In all events, we further comply with the requirements of both the US-EU Privacy Shield Framework and the Swiss-US Privacy Shield Framework with respect to such information. Our Privacy Shield compliance program is described generally here. In the following paragraphs we provide our Swiss and EU-based employees with the notice required by each Privacy Shield Framework, describe for them their choices and otherwise set out the specific ways in which we implement our Privacy Shield program with regard to EU HR Data:

Notice

We receive, process and use EU HR Data, and further transfer it to third parties to carry out our obligations under employment and benefit laws, to administer participation in our benefit, compensation and human resource plans and programs, for performance management, for compliance and for discipline reporting and investigation and purposes for which we have otherwise provided notice to data subjects. If we disclose EU HR Data:

- to a third party, other than a third party that is acting as an agent or processor to perform tasks on our behalf and under our instructions;

  or

- for purposes incompatible with those for which the EU HR Data was originally collected or subsequently authorized, then we take reasonable precautions to provide additional notice prior to the disclosure.

Choice

If we disclose EU HR Data to a third party, other than a third party that is acting as an agent or processor to perform tasks on our behalf and under our

instructions or for purposes incompatible with those for which the EU HR Data was originally collected or subsequently authorized, then we take reasonable precautions to offer the affected employee data subjects the opportunity to choose not to have their EU HR Data disclosed unless they have already authorized us to use the EU HR Data for such purposes. Where such information pertains to the special class of "sensitive information" described under the laws of the EU or Switzerland, including ideological views or activities, information on social security measures, or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings under the Swiss-US Privacy Shield Framework, we take reasonable precautions to offer an affirmative or explicit (i.e., "opt in") choice, before the EU HR Data is so disclosed.

Accountability for Onward Transfer

EU HR Data may be transferred to our third party service providers located in jurisdictions that have been deemed by the European Commission to have inadequate data protection laws. We only undertake such transfers after we have obtained assurances from such third parties that they subscribe to the core Privacy Shield Principles and satisfy our general data security and privacy expectations found here. Alternatively, we also may use written contracts requiring such third parties to provide at least the same level of privacy protection as is required by this policy. If we have knowledge that one of our third party agents is processing personal information in a manner contrary to this policy or any of the Privacy Shield requirements, we will take reasonable steps to prevent or stop such processing.

Security

At a minimum, we take reasonable precautions to protect EU HR Data in our possession from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. Please read here for more detail about the standards and expectations we set regarding physical and technical security for personal information, which standards apply to EU HR Data.

Data Integrity and Purpose Limitation

We only use the EU HR Data we collect in ways that are consistent with the purposes for which it was originally collected or for which we subsequently obtained authorization from the affected employees. We take reasonable steps to ensure that the information is reliable for its intended use, accurate, complete, and current. To accomplish this, we necessarily rely on our employees to exercise their Access rights to keep us apprised of any changes in their EU HR Data.

Access

If a Swiss or EU-based employee from whom we've collected data writes to us and asks to have access to EU HR Data, we will take all reasonable steps to ensure such access is granted. Obviously, the relevant information must be in our possession or under our reasonable control for us to do so. Once such access is granted, affected employees may further ask us to correct, amend or delete their information where it is determined to be inaccurate. There are, however, certain limitations to an employee's rights to such access and correction. These include situations where the burden or expense of providing access would be disproportionate to the risks to the employee's privacy, or where the rights of persons other than the employee would be violated.

Recourse, Enforcement and Liability

We implement processes and procedures to verify our compliance with this policy. If employees believe that we are not compliant, or if they have other complaints related to this policy or our conduct under it, we encourage those

employees to contact us. We commit to investigate and attempt to remedy all such complaints. If an employee complaint cannot be resolved, Tokio Marine shall cooperate and comply with the EU data protection authorities and/or the Swiss Federal Data Protection and Information Commissioner, as applicable, with respect to EU HR Data.

Changes to this Policy

We reserve the right to change or update this policy from time to time. Employees should check our site periodically for such changes since all information collected is subject to the policy in place at that time. Typically, we will indicate the effective/amendment date at the beginning of this policy. If we feel it is appropriate, or if the law requires, we'll also provide a summary of changes we've made near the end of the new policy.

Contacting Us

If employees have questions about our privacy policy or privacy practices, please contact the Privacy Office:

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