



## TRISTAR Privacy Notice

TRISTAR, its divisions, subsidiaries, and affiliates (collectively “TRISTAR” or “the Company” or “we,” “us,” or “our”) have created and updated this Privacy Notice (“Privacy Policy”) in compliance with applicable laws and to demonstrate our firm commitment to protecting individual privacy.

In this Privacy Notice, we identify the personal data that we may collect about you and how we may use that data. This Privacy Notice applies to any personal data you provide to TRISTAR and any personal data we may collect from other sources unless you are provided a more specific privacy statement at the time of the data collection. This Privacy Notice does not apply to any third-party websites, applications, or portals (“Sites”) linked to TRISTAR Sites. In this Privacy Notice, TRISTAR describes how we collect, use, disclose, transfer, store, retain or otherwise process your information when you (whether in your individual or business capacity) access or use, in any manner, any content, products, services or related activities (collectively “Services”), including through the Internet domains owned or operated by TRISTAR and its affiliates.

Your privacy is a major priority to TRISTAR and its affiliate companies. This Privacy Notice describes the ways in which we gather and protect information. It also includes what choices you have to control your information. When we refer to “you,” or “your,” we mean the person accessing the site. If the person accessing the site does so on behalf of, or for the purpose of, another person, including a business or other organization, “you” or “your” also means that other person, including a business organization. Please read this Privacy Notice carefully. By continuing to interact with our Services, including using any of our Sites and applications that link to this Privacy Notice or otherwise providing Personal Information to us, you agree and consent to the practices described in this Privacy Notice.

The Table of Contents will guide you through the sections containing our practices for the collection, use, disclosure, and retention of your personal data.



## TABLE OF CONTENTS

1.	How TRISTAR uses and protects personal data.....	4
A.	About TRISTAR.....	4
2.	How we process your personal data .....	5
A.	Individuals in scope of this Privacy Notice .....	5
B.	How we collect your personal data.....	5
C.	Personal data we collect .....	6
D.	How we use your personal data.....	7
E.	Legal basis for processing personal data.....	9
F.	Who we share your personal data with .....	10
G.	How we protect your personal data.....	11
H.	How we protect your personal data when sending it outside the USA .....	12
3.	How We Use Cookies .....	12
A.	Cookies Policy.....	12
B.	How to restrict cookies.....	13
4.	How We Use Information.....	14
A.	External partner advertising and analytics.....	14
B.	Linking sites .....	14
C.	Social media .....	15
D.	Marketing activities.....	15
E.	Profiling and automated decision-making .....	16
5.	Your Choices to Control Information.....	17
A.	Your personal data rights. ....	17
B.	How long we retain your information.....	17
6.	State Privacy Laws and Regulations .....	19
A.	California Privacy Policy.....	19
B.	Personal information we collect.....	19
C.	Categories of sources from which we collect personal information .....	21
D.	Our process of our personal information.....	21
E.	Disclosure of personal information .....	22
F.	No sales or sharing of personal information .....	22



- G. Use of sensitive personal information..... 22
- H. Your CPRA consumer rights..... 22
- I. Your right to access. .... 22
- J. Your right to data portability..... 22
- K. Your right to delete. .... 23
- L. Your right to correct. .... 23
- M. Your right to non-discrimination and no retaliation ..... 23
- N. Exercising your rights ..... 23
- 7. Verification process ..... 24
  - A. Response timing and format ..... 25
  - B. CPRA exemptions ..... 26
  - C. HIPAA Exemption ..... 26
  - D. Other California Privacy Rights..... 26
  - E. Notice of Colorado, Connecticut, Virginia, and Utah Privacy Rights ..... 27
  - F. Personal information we collect..... 27
  - G. Categories of sources from which we collect personal information ..... 27
  - H. Our processing your personal information ..... 27
  - I. Disclosure of personal information ..... 28
    - a) No sale of data or use of data for targeted advertising ..... 28
    - b) Your rights..... 28
    - c) Exercising your rights ..... 30
    - d) Authentication process ..... 30
    - e) Response timing and format..... 30
    - f) Right to appeal ..... 31
    - g) Exemptions ..... 31
- Revision History..... 33



## 1. How TRISTAR uses and protects personal data

### *A. About TRISTAR*

Headquartered in Long Beach, CA, TRISTAR was founded in 1987 by our president Thomas J. Veale. Originally named Topa Risk Services, the company began as an insurance program manager and medical malpractice claims administrator. Workers' compensation (WC) claims management services were added to our offerings in 1989. Growth and change followed, and in 1995 the company was renamed TRISTAR Risk Management. As managed care and benefits administration services were also added to our offerings, the organization grew into TRISTAR Insurance Group.

Today TRISTAR remains a privately held corporation. We are the largest independently owned third party property and casualty claims administrator in the US. We focus our operations in four divisions: property and casualty claims management (TRISTAR Claims Management Services), absence and benefits administration (TRISTAR Benefits Administrators), managed care and medical cost containment services (TRISTAR Managed Care), and loss control and risk assessment services (Aspen Risk Management). Each division provides services nationwide, and we have nearly 1000 employees across the country.

TRISTAR has branches across the United States in major metropolitan areas, with staff working in offices, virtually, in hybrid models, or onsite in client facilities, providing claims administration services for claims arising in all 50 states.

(WC Only) More than 80% of our property and casualty claims management business is workers' compensation, and nearly half of our clients are public entities. We serve a wide range of public entity clients, including school districts, cities, counties, states, public transportation systems, special districts, law enforcement agencies, and other municipal entities.

Ancillary services, including utilization review, bill review, nurse case management, and nurse triage services, are consolidated in various locations throughout the United States to improve services and lower costs, which can then be passed onto our clients.

## 2. How we process your personal data

### *A. Individuals in scope of this Privacy Notice*

This Privacy Notice provides information for those individuals whose personal data we process, including:

- Business contacts, such as brokers, (re)insurers, loss adjusters, experts instructed in relations to claims, service providers, suppliers, professional advisors, conference attendees, visitors to our offices, government officials and authorities.
- Customers, such as those in respect of insurance policies we place or self-insured programs we administer as part of our core business activities (e.g., parties covered under the policies, self-insured programs, potential beneficiaries of the policies or self-insured programs, claimants, and other parties involved in claims in respect of the policies or self-insured programs), and any other customers in relation to our various service offerings (e.g. employer sponsored health and benefit plans).
- Users of our Sites.
- Other individuals, such as those requesting or receiving our marketing information, making general inquiries, entering competitions or promotions, or whose images we use in marketing or are captured on CCTV.

### *B. How we collect your personal data*

We may collect your personal data in a few ways, which vary based on how you interact with us. The following summarizes our data collection sources:

- Directly from you or your authorized representative, such as when you provide your personal data to us, including from any of our Sites, surveys, live events, market research, and other direct communications and/or solicitations.
- From our clients and partners, such as commercial clients, (re)insurers, network partners, employers, benefit plan sponsors, benefit plan administrators, premium finance companies, health services providers, data/marketing providers and third-party service providers.
- Publicly available sources, such as social media platforms, property and assets registers, and claims and convictions records.
- TRISTAR affiliate companies.
- Government authorities, such as police and regulators.

- Background check and screening tools, such as insurance industry fraud prevention and detection databases, credit agencies and sanctions screening tools.
- Other third parties.

### *C. Personal data we collect*

We may collect the following types of personal data depending on the purpose of your interaction with us (e.g., as business contact, customer, claimant, insured):

- Basic personal and demographic information, such as your name, date of birth, age, gender, and marital status.
- Contact information, such as your address, telephone number and email address.
- Unique identifiers, such as identification numbers issued by government bodies or agencies (e.g., your national identifier number or social security number, passport number, ID number, tax identification number, driver's license number).
- Employment information, such as your job title, employer, employment status, salary information, employment benefits, employment history and professional certifications.
- Financial information, such as your bank account numbers, credit card numbers, brokerage account numbers, transaction information, tax information, details of your income, property, assets, investments, pension and benefits, debts, and creditworthiness.
- Policy information, such as our policy number, policy start and end dates, premiums, individual terms, claims history and claims data, mid-term adjustments, reasons for cancellation, risk profile and details of policy coverage.
- Claim information, such as claimant's relationship to policyholder/insured, and the date and particulars of such claim, including causes of death, injury or disability and claim number.
- Commercial information, such as records of your personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Events or meeting information, such as details about your visits to our offices (including CCTV), your interest in and attendance at events or meetings, audio recordings, photographs or videos captured during meetings, events, or calls with you.

- Special category data and sensitive personal data, such as data relating to your health (including protected health information), genetic or biometric data, sex life, sexual orientation, gender identity, racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership.
- Criminal records information, such as criminal charges or convictions, including driving offences, or confirmation of clean criminal records.
- Professional disciplinary information.
- Personal information received from background checks and sanctions screenings.
- Marketing information, such as your consent to or opt out from receiving marketing communications from us and/or third parties, your marketing preferences, or your interactions with our marketing campaigns and surveys, including whether you open or click links in emails from us or complete our surveys.
- Sites and communication usage information, such as your username, your password, other information collected by visiting our Sites or collected through cookies and other tracking technologies, including your IP address, domain name, your browser version and operating system, traffic data, location data, browsing time, and social media information, such as interactions with our social media presence.

#### *D. How we use your personal data*

Depending on the purpose of your interaction with us (e.g., as business contact, customer, claimant, insured), we may use your personal data to:

- Perform services for you or our clients.
  - Provide services and fulfill our contractual obligations, including providing services that you may not have personally requested but were requested by our client(s) and require us to interact, directly or indirectly, with you.
  - Facilitate and enable placement of policies and assist in the ongoing management of such policies, including premium management, renewals, adjustments, cancellations, claims management and settlement.
  - Provide various consulting, administration and actuarial services and claims administration.

- Advise on the management of our clients' business risks and opportunities, affairs, and insurance arrangements and on the administration of claims.
- Manage our business operations.
  - Enter business relationships and perform due diligence and background checks, such as fraud, trade sanctions screening, and credit and anti-money laundering checks.
  - Create, maintain, customize, and secure your account with us.
  - Maintain accounting records, analyze financial results, comply with internal audit requirements, receive professional advice, apply for and make claims on our own insurance policies, manage or dispute a claim and recover a debt.
  - Conduct data analytics, surveys, benchmarking, and risk modeling to understand risk exposures and experience, for the purposes of creating de-identified and/or aggregate industry or sector-wide reports, to share within TRISTAR's divisions, subsidiaries, affiliates, and with third parties.
- Communicate and market to you.
  - Communicate with you regarding your account or changes to our policies, terms, and conditions, respond to any inquiries you may have, and send you invitations for events or meetings.
  - Advertise, market, and promote our services or the services of others, including by email, LinkedIn, SMS, USPS, or telephone.
  - Send you newsletters, offers or other information we think may interest you, as well as offer and administer promotions.
  - Monitor usage of our Sites and personalize your experience with our Sites and the messages we send you to deliver content, product, and service offerings relevant to your interests, including targeted offers and ads through our Sites, third-party Sites, and via email, SMS, or text (with your consent, where required by law).
- Comply with legal obligations.
  - Comply with national security or law enforcement requirements, discover requests, or where otherwise required or permitted by applicable laws, court orders or regulatory authorities.
  - Exercise and defend ours, yours or third parties' legal rights.
- Monitor and prevent fraud or wrongdoing.
  - Maintain the safety, security, quality, and integrity of our products, services, systems, and data, detect security incidents, protect against inadvertent data loss, malicious, deceptive, fraudulent, or illegal activity,



- and debug or identify and repair errors that impair existing intended functionality.
- Monitor and ensure the safety and security of our premises, employees, and visitors.
- Improve our services.
  - Develop, enhance, expand, or modify our services through research and development.
  - Monitor, review, assess and improve our technology systems, including any Sites, and our content on social medial platforms.
  - Improve quality, training, and security (for example, with respect to recorded calls).
- Mergers and acquisitions
  - Facilitate commercial transactions, including a reorganization, merger, sale of all or a portion of our assets, a joint venture, assignment, transfer, or other disposition of all or any portion of our business, assets, or stock (including in connection with any bankruptcy or similar proceedings). Should such a sale or transfer occur, we will use reasonable efforts to ensure the entity to which we transfer your personal data agrees to use it in a manner consistent with this Privacy Notice.

If we intend to use your personal data for any other purpose not described in this Privacy Notice or which is not compatible with the purpose for which your personal data was collected, we will contact you and let you know of that purpose, which may include the need to satisfy our legal and regulatory obligations. Where we require your consent to the processing, we will request it in advance.

#### *E. Legal basis for processing personal data*

Local law and regulation may require us to have a legal basis to process your personal data. In most cases, our legal basis for processing your personal data will be one of the following:

- Legitimate Business Interest, such as seeking to and entering into or performing our contractual duties, maintaining our business records, keeping records of insurance policies we place, and analyzing and improving our business model and services. When using your personal data for these purposes, we ensure our business need does not conflict with the rights afforded to you under applicable laws.
- For the performance of a contract with you or to take steps at your request prior to entering into that contract.
- Compliance with legal obligations.



- Fraud detection or prevention.
- Consent, such as when we must obtain your consent to process your personal data.

When we process sensitive personal data, sometimes referred to as special category data, our legal basis will be one of the following:

- As required to establish, exercise, or defend legal claims.
- As necessary for insurance operations when it is in the substantial public interest, where applicable under local data protection laws.
- You have given us your explicit consent – where we receive sensitive personal data or special category data indirectly, the third party is responsible for obtaining your explicit consent to enable us to collect and use your data for the purposes described in this Privacy Notice.

#### *F. Who we share your personal data with*

We do not sell or rent to anyone the personal information you have provided to us, nor the personal information of minors under sixteen (16) years of age to third parties ([See COPPA Section](#)).

We may share your personal data within TRISTAR's group of companies for the purpose of your interaction with us, such as for the provision of our Services, general business operations, marketing, data analytics, surveys, benchmarking, and compliance with applicable laws.

We may also share your personal data with the following third parties for the purpose of your interaction with us:

- Professional Advisors, such as underwriters, actuaries, claims handlers and investigators, surveyors, loss adjustors/assessors, accident investigators, specialist risk advisors, pension providers or trustees, banks and other lenders (including premium finance providers), health professionals, health service providers, lawyers (including third party legal process participants), accountants, auditors, tax advisors, financial institutions, investment advisors and other fiduciaries and consultants.
- Business partners, such as customers, (re)insurance companies, brokers, other insurance intermediaries, claims handlers or other companies who act as insurance distributors.
- Providers of insurance brokering platforms.

- Service providers, such as IT software, security and cloud suppliers, finance and payment providers, marketing agencies, external venue providers, document management providers, telephone providers, debt collection agencies, background check and credit reference agencies.
- Fraud detection agencies who operate and maintain fraud detection registers.
- Industry bodies.
- Insurers who provide our own insurance.
- Regulators, public authorities, and law enforcement agencies, such as police, judicial bodies, governments, quasi-governmental authorities, and workers' compensation boards.
- Asset purchasers, such as those who may purchase or to whom we may transfer, our assets and business.

When we share personal data with third parties, we require those third parties (where applicable) to maintain a comparable level of protection of personal data as set out in this Privacy Notice by the use of contractual requirements or other means. On request and where required by law, we will confirm the name of each third party to which your personal data has, or will be, transferred. To the fullest extent permitted by applicable law, we disclaim all liability for the use of your personal data by third parties.

### *G. How we protect your personal data*

We use a range of organizational and technical security measure to protect your personal data, including the following:

- Restricted access to those who need to know for the purposes set out in our underlying agreement or this Privacy Notice.
- Firewalls to block unauthorized traffic to servers.
- Physical servers located insecure locations and accessible only by authorized personnel.
- Internal procedures governing the storage, access, and disclosure of your personal data.
- Additional safeguards as may be required by applicable laws in the jurisdictions where we process your personal data.

Please note that where we have given you (or you have chosen) a password, you are responsible for keeping the password confidential. Please do not share your password with anyone.



### *H. How we protect your personal data when sending it outside the USA*

Our business operations may include transmission of your personal data outside the USA to certain third parties, including our partners and service providers. This sharing of data allows us to provide you Services as set out in our underlying agreement or as otherwise indicated in this Privacy Notice. Transfers of personal data will be subject to appropriate safeguards to ensure an adequate level of protection and compliance with applicable law. Please contact us using the details provided under the [Contact The Privacy Office](#) section if you would like further information regarding the steps, we take to protect your personal data when sending it outside the USA.

## **3. How We Use Cookies**

### *A. Cookies Policy*

TRISTAR and our analytics vendors use server logs and automated data collection tools such as browser cookies, pixel tags, scripts and web beacons. These tools are used for analytics purposes to enable TRISTAR to understand how users interact with the Sites and Services. TRISTAR and our analytics vendors may tie the information gathered by these means to the identity of users.

Cookies are small text files placed on a computer or device while browsing the Internet. Cookies are used to collect, store and share bits of information about user activities. TRISTAR uses both session cookies and persistent cookies.

Session cookies are used to identify a particular visit to TRISTAR Sites and collect information about your interaction with the Sites. These cookies expire after a short time or when the user closes their web browser after using the Sites. TRISTAR uses these cookies to identify a user during a single browsing session, such as when you log into the Sites. This helps TRISTAR improve the Sites and Services as well as improve the users' browsing experience.

A persistent cookie will remain on a user's device for a set period specified in the cookie. TRISTAR uses these cookies to identify and recognize a specific user over a longer period. They allow TRISTAR to:

- Analyze the usage of the Sites (e.g., what links users click on) to improve our offering.



- Test different versions of the Sites to see which features or content users prefer to optimize the Sites.
- Provide a more personalized experience to users with more relevant content and course recommendations.
- Allow users to more easily log in to use the Sites and Services.

Examples of persistent cookies include: (i) preferences cookies to remember information about a user's browser and settings preference, such as preferred language – preference cookies make a user's experience more functional and customized, (ii) authentication and security cookies to enable a user to log in or stay logged in to access the Sites and Services, to protect user accounts against fraudulent log-ins by others and to help detect and protect against abuse or unauthorized usage of user accounts and (iii) functional cookies to make the experience of using the Sites and Services better, like remembering the sound volume level selected by the user.

TRISTAR uses tracking technology to; (i) determine if a certain page was visited or an email sent by TRISTAR was opened or clicked on by a user; and (ii) to customize the experience of individual users by recommending specific content.

We also use clear gifs in HTML-based emails sent to our users to track which emails are opened and clicked on by recipients. We may use the information we obtain from the cookie in the administration of the Sites, to improve the usability of the Sites and for marketing purposes. We may also use the information to recognize your computer when you visit our Sites, and to personalize our site for you.

Cookies and information captured through our Sites are stored for a certain retention period, however you can eliminate these cookies any time before the expiration date.

### *B. How to restrict cookies*

You can adjust the settings in your browser to restrict or block cookies that are set by the Sites (or any other website on the Internet). Your browser may include information on how to adjust your settings.

You can control and delete these cookies through your browser settings through the following:

- Google Chrome
- Mozilla Firefox
- Safari
- Opera



- Microsoft Internet Explorer
- Microsoft Edge
- Safari for IOS (iPhone and iPad)
- Chrome for Android

Please be aware that restricting cookies may impact the functionality of the Services. Most browsers allow you to refuse to accept cookies.

## 4. How We Use Information

### *A. External partner advertising and analytics*

We may use service providers to provide site metrics and other analytics services. These service providers may use cookies, web beacons and other technologies to collect information, such as your IP address, identifiers associated with your device, other applications on your device, the browsers you use to access our Sites and Services, webpages viewed, time spent on webpages, links clicked and conversion information (e.g., transactions entered into). This information may be used by TRISTAR and service providers on behalf of TRISTAR to analyze and track usage of our Sites and Services, to determine the popularity of certain content and to better understand how you use our Sites and Services. The service providers that we engage are bound by confidentiality obligations and other restrictions with respect to their use and collection of your information.

This Privacy Notice does not apply to, and we are not responsible for, third-party cookies, web beacons or other tracking technologies, which are covered by such third parties' privacy policies. For more information we encourage you to check the privacy policies of these third parties to learn about their privacy practices.

### *B. Linking sites*

The Sites contain links to other websites. TRISTAR is not responsible for the privacy practices or the content of such websites, including any websites that may indicate a special relationship or partnership with us (such as co-branded pages or "powered by" or "in cooperation with" relationships). We do not share information we gather with other websites or any other entities or individuals unless such sharing is disclosed to you in advance through this Privacy Notice. Other linked websites, however, may collect



personal information from you that is not subject to our control. To ensure protection of your privacy, always review the privacy policy of the websites you may visit by linking from the Sites. Please note that this Privacy Notice applies only to our Sites, and not to other companies' or organizations' websites to which we link.

For instance, information collected through Google Analytics is shared with Google and its partners who may combine it with other information you provided to them, or they collected from your use of their services. This information is stored in Google's servers according to their privacy practices.

### *C. Social media*

We may collect information from other sources, such as social media platforms that may share information about how you interact with our social media content. We do not control how your personal information is collected, stored, or used by third-party websites or to whom those websites disclose your information. You should review the privacy policies and settings on any social media website that you subscribe to so that you understand the information they collect and may be sharing. If you do not want your social media websites to share information about you, you must contact that website and determine whether it gives you the opportunity to opt-out of sharing such information. TRISTAR is not responsible for how these third-party websites may use information collected from or about you.

Further, our Sites may include social media features, such as the Facebook Like button. Our integration of these features may allow external social media to collect certain information, such as your IP address and which page(s) you are visiting when using our Sites and Services, and to set a cookie to enable that feature to function properly. Your interactions with these features are governed by the privacy policy of the company providing it.

### *D. Marketing activities*

We may, periodically, provide you with information about our products or Services or those of our partners that we think will be of interest to you. We may send you this information by email, LinkedIn, SMS, text, post, or we may contact you by telephone. We may also share your personal data with other TRISTAR group companies so that they can provide you with information about their products and Services we believe will be of interest to you. We ensure that our marketing activities comply with all applicable legal



requirements. In some cases, this may mean that we ask for your consent in advance of sending you marketing materials.

You can opt out of marketing communications from us at any time. For example, you can click on the “unsubscribe” link in our marketing emails to unsubscribe from those emails. Alternatively, please contact us using the details provided under the [Contact Us](#) section. In such circumstance, we will continue to send you service-related communications where necessary.

### *E. Profiling and automated decision-making*

Insurance market participants benchmark insured, beneficiary and claimant attributes and risk factors, and insured event likelihoods to determine insurance limits, insurance premiums, and fraud patterns. This means that we may compile and analyze data in respect of insureds, beneficiaries, and claimants to model such likelihoods. In doing so, we may use personal and commercial data to create the models and/or match that data against the models (profiling) to determine both the risk and the premium price based on similar exposures and risks. We also use this information to help us advise insurance companies about the typical levels of insurance coverage that our clients may have in place.

We will only make automated decisions about you where:

- Such decisions are necessary for entering into a contract (e.g., we may decide not to offer Services to you, the types or amount of Services that are suitable for you, or how much to charge you for Services based on your credit history or financial or related information we have collected about you);
- Such decisions are required or authorized by law (e.g., fraud prevention purposes); or
- You give your consent for us to carry out automated decision-making.

These automated decisions may have a legal or similar effect on you, namely, your eligibility for or access to products or Services.

We may also make automated decisions based on your personal data or browsing history to send you personalized offers, discounts, or recommendations, subject to any applicable local laws and regulations. These automated decisions will not have legal or similar effects for you.





Subject to local laws and regulations, you can contact us to request further information about our automated decision-making, object to our use of automated decision-making, or request that an automated decision be reviewed by a human being.

## 5. Your Choices to Control Information

### *A. Your personal data rights.*

Based on the jurisdiction in which you reside, and subject to permitted exemptions, you may have certain rights in relation to your personal data. We are committed to respecting your personal data rights.

You can exercise your rights by contacting us using the details provided in the [Contact Us](#) section. We will usually not charge you for processing these requests. There may be cases where we are unable to comply with your request (e.g., via a permitted exemption or where the request would conflict with our obligation to comply with other legal requirements). We will tell you the reason if we cannot comply with your request and we will always respond to any request you make.

### *B. How long we retain your information.*

We generally retain your information as long as reasonably necessary to provide you the Services or to comply with applicable law and in accordance with our document retention policy. To determine the appropriate retention period for personal information, we consider the amount, nature and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means and the applicable legal requirements. We may retain copies of information about you and any transactions or Services you have used for a period of time that is consistent with applicable law, applicable statute of limitations or as we believe is reasonably necessary to comply with applicable law, regulation, legal process or governmental request, to detect or prevent fraud, to collect fees owed, to resolve disputes, to address problems with our Services, to assist with investigations, to enforce other applicable agreements or policies or to take any other actions consistent with applicable law.

In some circumstances we may anonymize your personal information (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you. This allows the specific



information collected (name, email, address, phone number, etc.) to become anonymous, but allows TRISTAR to keep the transaction or engagement data. For example, TRISTAR will not be able to tell if John Smith registered for an event, but we will be able to tell that a person registered for an event and maintain headcount and transactional history. This will allow TRISTAR to maintain a level of information that helps us develop and improve our Sites and Services.

### Contact The Privacy Office

There are several ways to contact the Privacy Office.

To contact us if you need to report a privacy issue or if you have any questions about how we collect and process your personal data, you can:

- Call the Privacy Office at: 562-625-8242
- Write to the Privacy Office at:

TRISTAR

C/O Privacy Office

100 E Ocean Blvd, Suite 840

Long Beach, CA 90802

- Email the Privacy Office at: [Privacy@tristargroup.net](mailto:Privacy@tristargroup.net)
- Or submit a [Privacy Rights Request Form](#)

### Updates to this Privacy Notice

We may update this Privacy Notice from time to time. When we make updates, we will post the current version on our Sites and will revise the version date located at the end of the Privacy Notice. We encourage you to review this Privacy Notice periodically so that you will be aware of our current privacy practices.



## 6. State Privacy Laws and Regulations

### A. California Privacy Policy

The section (California Privacy Policy) relates solely to residents of the state of California, and for purposes of this section, “you” means residents of the state of California. This section will provide you with information about our Information Practices and your privacy rights under the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA) and applicable regulations (collectively referred to as “CPRA”). Any terms defined in the CPRA have the same meaning when used in this section.

### B. Personal information we collect.

TRISTAR collects information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California consumer or household (“CPRA Covered Personal Information” or “personal information”). CPRA Covered Personal Information does not include personal information that has been de-identified or aggregated, or that is publicly available information from government records.

We have collected the following information categories of CPRA Covered Personal Information from consumers (as that term is defined in the CPRA) within the last twelve (12) months:

Personal Information Examples	Category	Collected
A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver’s license number, demographic information, passport number, or other similar identifiers.	Basic Identifiers.	Yes
A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, medical information, or health insurance	Personal information listed in the California Customer Records statute	Yes

Personal Information Examples	Category	Collected
information. Some personal information included in this category may overlap with other categories.	(Cal. Civ. Code § 1798.80(e)).	
Age (40 years or older), race, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran, or military status.	Protected classification characteristics under California or federal law.	Yes
Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	Commercial Information	Yes
Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	Biometric information.	Yes
Browsing history, search history, information on your interaction with a site, application, or advertisement.	Internet or other similar network activity.	Yes
Physical location or movements	Geolocation data.	Yes
Audio, electronic, visual, thermal, olfactory, or similar information.	Sensory data.	Yes
Occupation, title, employer information, current or past job history or performance evaluations.	Professional or employment related information	Yes

Personal Information Examples	Category	Collected
Education records directly related to a student maintained by an education institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Yes
Profile reflecting a person’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	Inferences drawn from other personal information	Yes
Social Security number, driver’s license, state identification or passport numbers; account log-in, financial account, debit or credit card number in combination with any required security or access code, password or credentials allowing access to an account; process geolocation data; racial or ethnic origin, religious or philosophical beliefs or union membership, content of mail, email and text messages unless business is the intended recipient; genetic data; processing of biometric information for the purposes of uniquely identifying a consumer; personal information collected and analyzed concerning your health.	Sensitive Personal Information	Yes

*C. Categories of sources from which we collect personal information.*

You have the right to know the categories of sources from which we collect your personal information. We make this information available to you in the [How we Collect Your Personal Data](#) section of this Privacy Notice.

*D. Our process of our personal information*

You have the right to know how we process and use your personal information. We make this information available to you in the [How We Use Your Personal Data](#) section of this Privacy Notice.



*E. Disclosure of personal information*

You have the right to know if we share your personal information with any third parties and the categories of those third parties. We make this information available to you in the [Who We Share Your Personal Data With](#) section of this Privacy Notice.

*F. No sales of sharing of personal information*

We do not sell personal information for monetary or other consideration, and we do not share your personal information for cross-context behavioral advertising (as defined in the CPRA). We do not sell or share the personal information of consumers under 16 years of age. We make this information available to you in the [Who We Share Your Personal Data With](#) section of this Privacy Notice.

*G. Use of sensitive personal information*

We do not use or disclose sensitive personal information for purposes other than those specified in section 7027, subsection (m) of the CPRA regulations and we do not collect or process sensitive personal information for purposes of inferring characteristics about you.

*H. Your CPRA consumer rights*

Where we are acting as a business (as opposed to a service provider as those terms are defined in the CPRA), you have the following rights:

*I. Your right to access.*

You have the right to request that we disclose the categories of personal information we collected about you, the categories of sources for the personal information we collected about you, our business or commercial purpose for collecting your personal information, the categories of third parties with whom we share your personal information and the specific pieces of personal information we collect about you.

*J. Your right to data portability*

You have the right to obtain a copy of your data in a portable format, and to the extent technically feasible, readily usable format that allows you to transmit the data to a third party.

*K. Your right to delete.*

You may have the right to request that we delete your personal information where we act as a business. This right is subject to several exceptions and we may deny your deletion request if retaining the information is necessary for us or our service provider to:

1. Complete the transaction for which we collected the personal information and take actions reasonably anticipated within the context of our ongoing business relationship with you or our client;
2. Detect bugs or errors in our Sites, detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
3. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us;
4. Comply with a legal obligation; or
5. Make other internal and lawful uses of that information as permitted by law or that are compatible with the context in which we collected it.

*L. Your right to correct.*

We take reasonable steps to ensure that information we hold about you is accurate and complete. However, you have the right to request that we correct any inaccurate personal information that we have about you.

*M. Your right to non-discrimination and no retaliation*

We will not discriminate or retaliate against you for exercising any of your rights under the CCPA, including we will not deny you goods or services, charge you different prices for goods or services, provide you a different level or quality of goods or services, or suggest that you will receive a different price for goods or services or a different level of quality of goods or services.

*N. Exercising your rights*

You may exercise your rights to know, delete and correct as described above by submitting a verifiable request to us by either:

- Calling the Privacy Office at 562-625-8242
- Writing to the Privacy Office at:



TRISTAR  
C/O Privacy Office  
100 E Ocean Blvd., Suite 840  
Long Beach, CA 90802

- Emailing us at: [Privacy@tristargroup.net](mailto:Privacy@tristargroup.net)
- Or, by submitting a [Privacy Rights Request Form](#)

## 7. Verification process

We are only required to fulfill verifiable requests. Only you, you as a parent or a legal guardian on behalf of a minor child, or your authorized agent may make a verifiable request related to personal information.

If you submit your request through an authorized agent, we may require you to provide your agent with written permission to do so and verify your identity. We may deny any request by an authorized agent that does not submit proof that the agent has been authorized by you to act on your behalf.

- For requests for access to categories of personal information, we will verify your request to a “reasonable degree of certainty.” This may include matching at least two data points that you would need to provide with data points we maintain about you and that we have determined to be reliable for the purposes of verification.
- For requests for specific pieces of personal information (portability request), we will verify your request to a “reasonably high degree of certainty.” This may include matching at least three data points that you would need to provide with the data points we maintain about you and that we have determined to be reliable for the purposes of verification. We will also require you to submit a signed declaration under penalty of perjury that you are the consumer whose personal information is the subject of the request.
- For requests to delete, we will verify your request to a “reasonable degree” or a “reasonably high degree of certainty” depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized agent.

We will use the personal information you provide in a request only for purposes of verifying your identity or authority to make the request.





#### A. *Response timing and format*

We will respond to a verifiable request within forty-five (45) days of its receipt and will notify you within those forty-five (45) days if we require more time to respond and the reason for the additional time.

If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option.

Any information we provide in response to a verified request will include information we have collected about you on or after January 1, 2022, including beyond the 12-month period preceding our receipt of the request, unless doing so proves impossible or would involve disproportionate effort, or you request data for a specific time period. (Note that the law prohibits us from disclosing at any time a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or any unique biometric data.)

If we cannot comply with a request or a portion of the request, we will include the reason in our response. If we deny your request on the basis that it is impossible or would involve a disproportionate effort, we will explain our reasons, such as the data is not in a searchable or readily accessible format, is maintained for only legal or compliance purposes, or is not sold or used for any commercial purpose and our inability to disclose it, delete or correct it would not impact you in any material manner.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Please note that in certain cases we may collect your personal information as a service provider (as opposed to a business, as those terms are defined in the CPRA) pursuant to a contract we have with a commercial client (the CPRA business) to provide a service. In such a case, we are required to collect and process your information only based on the instructions received from the business. Should you direct your requests to exercise your rights to us, we may be required to share your request with the business, who is the party responsible under the CPRA for



receiving, verifying, and responding to your requests, or we may direct you to make your request directly to the business.

### *B. CPRA exemptions*

This section (California Privacy Policy) does not apply to the following data which is exempt from the CPRA, including but not limited to: medical information governed by the California Confidentiality of Medical Information Act (CMIA); protected health information collected by a covered entity or business associate governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), or personal information collected, processed, sold, or disclosed pursuant to certain sector-specific laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994 (DPPA).

### *C. HIPAA Exemption*

The California legislature has exempted health providers and insurers already under HIPAA. The HIPAA exemption in CCPA only applies to PHI or ePHI (electronic personal health information). Everything else is subject to the CCPA interpretation.

- Part 1 of the CCPA HIPAA exemption (California Civil Code 1798.145(c)(1)(A)): PHI collected for the treatment, payment, or healthcare operations would qualify for the CCPA HIPAA exemption. However, health information that is collected for other purposes would not fall under the CCPA HIPAA exemptions and would be subject to the stricter privacy laws set forth by the CCPA. Workers Compensation is not subject to the HIPAA regulation.
- Part 2 of the CCPA HIPAA exemption (California Civil Code 1798.145(c)(1)(B)): A covered entity may qualify for the CCPA HIPAA exemption under part 2. Part 1 exempts PHI, while Part 2 exempts providers, under certain circumstances. A covered entity governed by the HIPAA privacy, security, and breach notification rules, is exempt from the CCPA to the extent the covered entity properly safeguards PHI under HIPAA. This means that if a covered entity is not compliant with one or more HIPAA regulations, the covered entity is not in complete compliance with the CCPA.

### *D. Other California Privacy Rights*

California's "Shine the Light" law permits users of our Sites who are California residents to request certain information regarding our disclosure of personal information to affiliates and other third parties for their direct marketing purposes. To make such a request, please send an email to [Privacy@tristargroup.net](mailto:Privacy@tristargroup.net).



### *E. Notice of Colorado, Connecticut, Virginia, and Utah Privacy Rights*

The section (Notice of Colorado, Connecticut, Virginia, and Utah Privacy Rights) relates solely to residents of the States of Colorado, Connecticut, Virginia, and Utah, and provides you with information about your privacy rights under the Colorado Privacy Act, the Connecticut Data Privacy Act, the Virginia Consumer Data Protection Act, and the Utah Consumer Privacy Act.

This section shall be effective for the residents for those States on the dates set forth below.

Effective January 1, 2023, for residents of the State of Virginia

Effective July 1, 2023, for residents of the States of Colorado and Connecticut

Effective December 31, 2023, for residents of the State of Utah

For purposes of this section, “residents,” “consumers” or “you” means individuals of those states who are acting in their individual or household context. This section does not apply to individuals acting in their commercial or employment context.

### *F. Personal information we collect*

You have a right to know the categories and types of personal information we collect about you. We make this information available in the [Personal Data We Collect](#) section of our Privacy Notice.

### *G. Categories of sources from which we collect personal information*

You have a right to know the categories of sources from which we collect your personal information. We make this information available to you in the [How We Collect Your Personal Data](#) section of our Privacy Notice.

### *H. Our processing your personal information*

You have the right to know how we process and use your personal information. We make this information available to you in the [How We Use Your Personal Data](#) section of our Privacy Notice.

For residents of the State of Virginia, to the extent that we maintain de-identified data, we take reasonable measures to ensure that de-identified data cannot be associated with a natural person, we publicly commit to maintaining and using de-identified data without



attempting to re-identify the data, and we contractually obligate any recipient of the data to comply with the same obligations.

### *1. Disclosure of personal information*

You have the right to know if we share your personal information with any third parties. We make this information available to you in the [Who We Share Your Personal Data With](#) section of our Privacy Notice.

#### *a) No sale of data or use of data for targeted advertising*

We do not sell your personal information and we do not use your data for targeted advertising (as that term is defined by your applicable State law). We may send you advertising in response to your request for information or feedback or based on your activities with our Sites, including your search queries and visits to our Sites. However, we will not send you targeted advertising based on your activities across non-affiliated Sites to predict your preferences or interests.

#### *b) Your rights*

Where we act as the Controller of your personal information (as opposed to a Processor as those terms are defined in your applicable State law), you have the right to submit a request to us for the following:

Your right to access.

You have the right to know if we process your personal information and have access to such information and certain details of how we use it.

Your right to correct.

We take reasonable steps to ensure that information we hold about you is accurate and complete. However, you have the right to request that we correct any inaccurate information personal information that we have about you.

Your right to delete.

You may have the right to request that we delete your personal information where we act as a controller. This right is subject to several exceptions, and we may deny your deletion request if retaining the information is necessary for us or our processors to:

1. Complete the transaction for which we collected the personal information and take actions reasonably anticipated within the context of our ongoing business relationship with you or our client;



2. Detect bugs or errors in our Sites, detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
3. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us;
4. Comply with a legal obligation; or
5. Make other internal and lawful uses of that information as permitted by law or that are compatible with the context in which we collected it.

#### Your right to restriction of processing (opt-out)

You have the right to opt-out of processing your personal information for purposes of profiling in furtherance of any automated processing of your data that produce legal or similarly significant effects concerning you. To opt-out complete and submit the [Privacy Rights Request Form](#). (This right only applies to residents of the States of Colorado, Connecticut, and Virginia.)

#### Your right to data portability

You have the right to obtain a copy of your data in a portable, and to the extent technically feasible, readily usable format that allows you to transmit the data to a third party.

#### Your right to non-discrimination and no retaliation

We will not discriminate or retaliate against you for exercising any of your rights, including but not limited to, by denying you goods or services, charging you different prices for goods or services, or providing you a different level or quality of goods or services.

#### Your right to restrict the processing of sensitive information

Unless we are processing your sensitive information pursuant to any of the legal exemptions listed in Section Seven (7) below or as otherwise allowed by law:

- For residents of the States of Connecticut, Virginia, and Colorado, we will not process your sensitive information without first obtaining your consent; and
- For residents of the State of Utah, we will not process your sensitive personal information without providing you with notice and an opportunity to opt out.



#### c) Exercising your rights

You may exercise your rights described above by submitting a request to us by either:

- Calling the Privacy Office at: 562-625-8242
- Writing to the Privacy Office at:

TRISTAR

C/O Privacy Office

100 E Ocean Blvd, Suite 840

Long Beach, CA 90802

- Emailing the Privacy Office at: [Privacy@tristargroup.net](mailto:Privacy@tristargroup.net)
- Or, by submitting a [Privacy Rights Request Form](#)

#### d) Authentication process

We will only fulfill a request when we can verify your identity and confirm that you are authorized to make such a request.

Only you, you as the parent or legal guardian on behalf of your minor child, or your authorized agent, guardian or conservator may make a request related to personal information. If an authorized agent, legal guardian, or conservator submits the request, we may require your written permission to do so and may require additional information to authenticate your identity. We may deny a request by an authorized agent, legal guardian or conservator who does not submit proof of authorization to act on your behalf.

#### e) Response timing and format

We will respond to an authenticated request within forty-five (45) days of its receipt and will notify you within those forty-five (45) days if we require more time to respond and the reasons for the additional time.

If you have an account with us, we will deliver our written response to the account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option.

If we cannot comply with a request or a portion of the request, we will include the reasons in our response.



For residents of the States of Colorado, Connecticut, and Utah, you may make one request within a twelve-month period at no charge. For residents of the State of Virginia, you may make a request up to two (2) times within a twelve (12) month period at no charge. We reserve the right to charge a fee to process or respond to any request that we consider excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

#### f) Right to appeal

You have the right to appeal our decision within a reasonable period of time after receipt of our response. You may appeal our decision by sending us an email to [Privacy@tristargroup.net](mailto:Privacy@tristargroup.net). We will respond to your appeal within sixty (60) days of receipt (forty-five (45) days of receipt for residents of Colorado) and will inform you of any decisions and the reasons for such decisions.

Please note that in certain cases we may collect your personal information as a processor (as opposed to a controller, as those terms are defined in your applicable State privacy law) pursuant to a contract we have with a commercial client (the controller) to provide a service. In such a case, we are required to collect and process your information only based on the instructions received from the controller. Should you direct your requests to exercise your rights to us, we may be required to share your request with the controller, who is the party responsible under your applicable State privacy law for receiving, authenticating, and responding to your requests.

#### g) Exemptions

This section (Notice of Colorado, Connecticut, Virginia, and Utah Privacy Rights) does not apply to certain entities and data that are exempt from your applicable State privacy law, including but not limited to the following: covered entities, business associates and protected health information governed by the:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH);
- Financial institutions and personal information subject to the Gramm-Leach-Bliley Act (GLBA); and
- Personal information collected, processed, sold, or disclosed pursuant to certain sector-specific privacy laws, including the:
  - Fair Credit Reporting Act (FCRA), the
  - Family Educational Rights and Privacy Act, the
  - Farm Credit Act, and the
  - Driver' Privacy Protection Act of 1994 (DPPA).



## Children's Online Privacy Protection Act (COPPA) compliance and related information

The Children's Online Privacy and Protection Act (COPPA) regulates online collection of information from persons under the age of 13. It is our policy to refrain from knowingly collecting or maintaining personal information relating to any person under the age of 18. If you are under the age of 18, please do not supply any personal information through the Sites. Parents and legal guardians shall ensure that their children do not transmit any personal data through our Services or websites without permission. If personal data has been transmitted by children, please inform us immediately using the information provided under the [Contact the Privacy Office](#) section so we can remove such information from our files.





## Revision History

<i>Version</i>	<i>Comment</i>	<i>By:</i>	<i>Date:</i>
<i>1.0</i>	<i>Reviewed and updated policy</i>	<i>TRISTAR Council</i>	<i>6/2023</i>