Workforce Privacy Policy

We are committed to protecting the privacy and security of the information we collect and to being transparent about the purposes for which we use your information. This statement sets forth our policies and practices regarding the collection, protection, disclosure, and use of information collected as part of one or more workforce-related processes.

Scope

This Workforce Privacy Policy is being provided by Tailored Brands, Inc., the parent company of popular clothing brands such as The Men's Wearhouse, Jos. A. Bank, K & G Fashion Superstore, and Moores. For employment-related purposes, all applicants, employees, and relevant contractors of these brands and other subsidiaries of Tailored Brands, Inc. (the "Company") are in scope of this Workforce Privacy Policy.

More specifically, the information provided here is applicable to individuals who are involved in recruitment activities, applying for employment, have been hired, or were previously a member of the Company's workforce, including spouses/ domestic partners and dependents of current or former workforce members, when spouse/domestic partner and dependent information is necessary to complete an employment-related process. For purposes of this Policy only, "workforce" and "employment" include the above-identified individuals and groups, individuals who are serving on a Tailored Brands, Inc. Board of Directors, and individuals who are performing services for the Company in a contractor role.

For all other consumers, the collection, protection, disclosure, and use of your information is described in our customer Privacy Policy.

Personal Information

The Company may collect personal information (information that can be used to identify you as an individual), including sensitive personal information, as described further in this Policy. We collect and use this information only as permitted or required by, and in compliance with, law.

Collection methods

Most personal information is collected directly from you, including the device you use to access our website(s), or from others you have authorized to provide information to us on your behalf. However, during regular recruitment activities we may leverage third-party sources including social media platforms (such as LinkedIn) and websites (such as job boards) to collect publicly available personal information

about prospective and current candidates. The public availability and use of your personal information by these social media and third-party websites are discussed in their respective privacy policies.

Disclosure of Personal Information

For all categories of information discussed below, information is disclosed:

- To our service providers: To fulfill your request or to complete an operational function for the Company, such as administering benefits.
- To government agencies and regulators: To demonstrate the Company's compliance with various laws and regulations.
- For a legal proceeding or action: Information may be disclosed as required by a legal proceeding, litigation, or subpoena.
- To a buyer, potential buyer, or other successor to our business during negotiations of or in connection with a merger, sale of company assets, financing, or acquisition of all or a portion of our business by another company.

Additional disclosures may be necessary, as noted within specific categories below.

Categories of Personal Information

When you apply to join our team, or over the course your employment, we may collect and use the following categories of personal information.

- Identifiers
    - What we collect:
        - contact information, including name, alias and other names, email address, telephone or mobile phone number, and postal address
        - Social Security Number, driver's license number or state ID card number, and passport number.
        - Dependent information, to administer Company-sponsored benefits
    - How it's used: To ensure that we have the correct information to contact you, to verify your identity and employment/benefit eligibility, for tax reporting, or to provide you access to our Company HR systems.
    - Additional disclosures: Basic identifying information, such as name and contact information, may be disclosed to others, including but not limited to:
        - Meeting organizers, as an attendee for virtual or live events
        - Other Company employees, as part of an internal employment profile(s)
- Protected Classifications
  Tailored Brands, Inc. is an Equal Opportunity Employer.

- What we collect: personal information related to protected classes, such as race, age, sex/gender, and ethnicity.
- How it's used: To fulfill legal requirements, such as reporting on the demographic makeup of our workforce, to complete background checks, verify citizenship status, complete internal pay equity studies, or to determine eligibility for certain benefits.

- Commercial Information

  Information related to your commercial affairs, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
  - What we collect:
    - Expense reimbursement—We will request itemized receipts of your purchases.
    - Background checks—This process may reveal information related to previous criminal convictions or items of concern for employment.
    - Garnishment actions—If any personal legal proceedings result in liens or other garnishment actions being issued against you, we may be required to collect and/or disclose additional information about you, your employment status and compensation, and judgment details related to the garnishment action as permitted by applicable law.
    - Adoption assistance—Reimbursement under our adoption assistance benefit will necessitate itemized receipts to prove that expenses were made for qualifying purposes.
  - How it's used: This information may be requested or collected to ensure compliance with Company policy or regulatory obligations. This information is also necessary to reimburse our workforce for covered expenses incurred.
- Biometric Information

  Certain applications that you have access to as part of your employment relationship with the Company may allow for use of biometrics for more expedited authentication. In these cases, the Company does not collect the biometric information but instead relies on a service provider to determine authenticated access.
- Internet or electronic network activity
  - What we collect:
    - Sign-In and Device Information—username and password, account name or number, and other online or device identifiers
    - Information regarding a web visitor's interaction with our career site, including use of social media 'share' functionality
    - Silent monitoring-- All activities conducted while on Company premises or while using Company equipment, including browsing and search history and information regarding interactions with websites and applications, our systems, and networks, are subject to monitoring.

    For more information, please review our Acceptable Use Policy, Employee Handbook, and/or consultant Code of Ethics and Business Conduct, as applicable.

- How it's used: For research, to gauge user interaction with our site(s), for security and troubleshooting, to validate security access is appropriate, and to ensure that our workforce is using resources wisely and not putting our Company at risk.

- Education Information
  - What we collect:
    - History—details about your education, such as the name of any educational institutions you attended, the location, years attended, and degrees obtained.
    - Tuition assistance—if you are eligible, and request to take advantage of our tuition assistance program, we will collect information from you regarding your enrollment, degree progress, and transcripts.
  - How it's used: To validate that you have the necessary educational qualifications to perform the job responsibilities and to ensure compliance with the Company's policies.
- Professional and Employment-Related Information
  - What we collect:
    - History—details about your previous employment, including any licenses or training to perform specific roles. This may be learned from you or from a background check.
    - Union membership—to understand if your background and employment relationship with us requires specialized oversight and treatment
    - Military service—If you request to take a leave from your employment with the Company to fulfill military service orders, we will request to obtain details regarding your orders for documentation purposes. Military service information may also be requested to determine a potential tax credit for the Company.
  - How it's used: To validate that you have the necessary experience and credentials to perform your assigned role, or to document compliance with Company policy.
- Audio, Electronic, Visual, Thermal, Olfactory, Similar Information
  - What we collect:
    - Health related information—temperature checks and other screening for work/health safety.
    - Audio information—in the form of voice/call recordings, for those workforce members who interact with customers in our contact center(s).
    - Silent monitoring-- All activities conducted while on Company premises or while using Company equipment, including email, are subject to monitoring.
  - How it's used: To ensure quality service, protect the Company and members of its workforce, and conduct investigations.
- Geolocation Data
  - What we collect: badge access, location and movement information for any driver roles, and IP address, which is registered to a geographic location but not a specific residential address.
  - How it's used: to ensure that certain records and restricted areas are accessed only by authorized persons and devices; any use of precise geolocation is for security validation only. For mobile applications used for employment purposes, such as Mobile Device

Management, tracking activity may be enabled by the employee on their device but it is not required that employees do so. Vehicle, and its driver's, movement and location information are used to ensure safe and responsible operation of Company vehicles.

- Other types of personal information

  This category covers personal information not included in other categories, such as signature, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.
  - What we collect:
    - Financial Information—bank account, billing address, and information about your income and account balances, for specific items such as your corporate-issued credit card or prepaid debit card usage.
    - Medical/health information—requests or claims you make under the Family and Medical Leave Act, Americans with Disabilities Act, workers compensation statutes, or OSHA. Information collected could also relate to a public health matter, such as pandemic preparedness.
  - How it's used: To provide payroll and other expense reimbursement directly to your bank accounts, as well as to meet legal requirements and ensure compliance with Company policies.
  - Exclusions: While the Company does provide employer-sponsored health, life, and disability insurance to specific workforce members, the Company does not receive any identifiable health information regarding workforce, spouse/domestic partner, or dependent medical care or payment for care.
- Inferences drawn to create a profile

  We may collect any or all the information above to create an employment profile for you.
  - What we collect: your preferences, aptitudes, abilities, attitudes, or behaviors that we can determine from the information you provide, background check results, performance or quality assurance reviews, and/or an analysis of data related to your Company work history and sales practices, as applicable.
  - How it's used: to ensure that we have individuals in the roles that best align with their skills and we, as an employer, can assure our regulators that those members of our workforce who represent the Company have the necessary skills, training, and values. This information may also be used by us or our third-party service providers to automatically suggest roles that align to your work experience and skill set.
- Sensitive Personal Information

  Sensitive Personal Information is a subset of personal information described previously. This definition generally includes one or more of the following examples: (A) Social Security Number (SSN), driver's license, state identification card, or passport number; (B) account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) precise geolocation; (D) racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) the contents of mail, email, and text messages, unless the business is the intended recipient of the communication; (F)

genetic data; (G) biometric information; (H) health information; or (I) sex life or sexual orientation.

As part of your employment relationship with the Company, we may collect one or more of these data elements, as is discussed in relevant categories above. This information is used and disclosed only for legitimate business purposes, as prescribed by law, and not to discriminate against individuals.

- Anonymous information
  On occasion, aggregate and anonymous data about our workforce are shared for analysis and research purposes. This could include, for example, industry comparison studies regarding compensation or an independent evaluation of key-employee insurance coverage.

Update your personal information

For all workforce members, it is important that you keep your contact information current. Even post-termination, it is important to keep your contact information current so that any benefits you are entitled to can be administered.

By accessing our HR system's self-service options, available to you via the Thread, you can update your contact and pay information, such as address, email address, phone number, work location, and direct deposit accounts. Please note that some of these actions may require additional validation by the Company before changes can become effective.

You can also update your benefit records by logging into our external vendor benefit management sites to manage your 401k or your life insurance.

For all other updates, please contact the Tailored Brands Human Resources at:

Phone: 281-776-7000

Email: MyHR@Tailoredbrands.com

Personal Information Security and Retention

The Company has standards of security to protect your data by putting in place physical, technical and administrative safeguards. The technology we use to protect your data is reviewed and improvements are implemented as needed.

Authorized employees and representatives are permitted to access and use data about you for approved business purposes. All members of our workforce must complete all required training to ensure they understand and follow established policies and laws when using your data. Furthermore, as it relates to

Social Security Numbers we will (1) protect the confidentiality, (2) prohibit unlawful disclosure, and (3) limit access.

Your information may be accessible by third-party vendors for the purpose of enabling them to store such data in connection with the permitted uses of your information under this Privacy Policy. Our third-party providers have an obligation to maintain the confidentiality of the information, except where disclosure is required by law.

Information is retained only for so long as reasonably necessary for the purposes set out above, in accordance with applicable laws. More specifically, we will retain your information while you are actively employed with us, plus seven (7) years. However, if you are a prospective employee, also referred to as a candidate, who is not ultimately hired to fill a role, we will only retain your personal information for three (3) years from the date that you applied.

Further, if you are an employee or former employee who obtained or is entitled to any medical or retirement benefits from us, we are legally required under ERISA to retain certain personal information permanently. These benefit services are managed by third-party service providers whom you can contact for ongoing maintenance of your accounts regardless of your current employment status with us.

Please note that, for members of our workforce who reside outside of the United States, including Canada, your personal information will be processed in the United States, where our servers are located. By applying for a job or accepting employment with us, you acknowledge that your information is protected by this Privacy Policy, and you consent to the transfer of personal information to the United States.

Information for California residents

The following sections apply to those California residents who are considered consumers under the California Privacy Rights Act—you have the right to know about the personal information we collect, use, and disclose.

- Sale of Personal Information. We do not sell the personal information of any member of the California workforce.
- Sharing Personal Information. We do not share, for purposes of cross-contextual behavioral advertising, any personal information of our workforce.
- Disclosure of Personal Information. All categories of personal information may be disclosed for a business purpose. Generally, this involves sharing under the following circumstances: auditing, compliance with a regulatory or other legal inquiry, detecting and preventing security incidents, technical functionality improvements, business succession, and third-party service providers who perform services on the Company's behalf, such as providing benefits.
- Minors under 16. We do not knowingly collect, use, or sell the personal information of minors under the age of 16 years of age.

- Rights Granted. Residents of California also have the following rights available to them, regarding personal information collected from you or collected about you from other sources. You, or your designated authorized agent, may elect the following:
    - Request that we provide you with specific pieces of personal information we have collected about you, which we will comply with unless we have a legal exception that allows us to deny your request.
    - Request that we disclose to you the categories of information we collected about you, who we collected that information from, how we used it, and who we have disclosed it to.
    - Request the deletion of personal information we collected about you, which we will comply with unless it is necessary for us to retain the information, in accordance with exceptions provided by law.
    - Request us to correct inaccurate information we have about you. Specific details how to make this request are available in an earlier section of this Policy.

  To make any of the above requests, please click here or call us at 281-776-7000.

- Antidiscrimination. Rest assured that we will not discriminate against you if you choose to exercise any rights prescribed to you by law.
- Authorized Agents. While an authorized agent may act on behalf of a California consumer, we may request written permission from the employee before honoring any requests made by an authorized agent. Any identity verification, noted below, will still need to be completed by the employee directly.
- Verification. We will conduct email authentication to ensure that requests were not made by a robot. If there is a need to verify your identity further, prior to releasing information in accordance with your request, we will contact you via email, through our consumer rights portal, or at the phone number you provided in your request submission. At that time, we will conduct additional knowledge-based authentication or request certain documentation to ensure that only those people who have a legal right to obtain information can do so.

Cookies and tracking options

Cookies: Certain parts of our career website(s) uses cookies and related technologies. Cookies are a technology storage mechanism. Specific pieces of information, some of which may be personal, such as IP address, are contained within a cookie. Most often though, the cookie will contain an anonymous unique identifier given to your web browser by a web server. The browser stores the cookie on your device. The cookie, and any information contained within it, is sent back, via a web beacon, to the server each time your browser requests that site. The information collected by or through the cookie might be about you, your preferences, or your device, but mostly cookies are used to make the sites work as you would expect.

You are free to set your device or Internet browser settings to decline nonessential cookies, but by doing so, you may not be able to use certain features on our website or take full advantage of all our offerings. Essential cookies cannot be declined because they are required for the website to function properly and for us to ensure the security of the website. Please refer to your device's settings or your Internet browser's "Help" section for more information on how to delete and/or disable your device or browser from receiving cookies. Please note that your browser settings only apply to the web browser you use at the time of making those setting choices, so you must adjust the setting of each web browser on each computer you use. Once you opt out, if you delete your browser's saved cookies, you will need to opt out again.

Do Not Track and Opt-Out Preference Signals: Historically, some mobile and web browsers transmitted "do-not-track" signals. Because of differences in how web browsers incorporate and activate these features, it is unclear whether users intend for these signals to be transmitted, or whether they even are aware of them, therefore, we do not act in response to these signals.

However, new technology, typically referred to as an "opt-out preference signal" or Global Privacy Control (GPC), has been developed. The purpose of an opt-out preference signal is to provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt out of sale/sharing of their personal information. Through an opt-out preference signal, a consumer can opt out of sale and sharing of their personal information with all businesses they interact with online without having to make individualized requests with each business. Because we do not sell or share your personal information, we will not honor the opt-out preference signal at this time.

We will not discriminate against you for exercising your rights and choices, although some of the functionality and features available on the Service may change or no longer be available to you. Any difference in the Services is related to the value provided.

Changes to this Privacy Policy

We will update this Policy from time to time to ensure it accurately describes how we use your information. When we do so, we will update the "Last Revised" date below. We recommend that you review this Policy from time to time for the latest information. If we change our practices in a material way, we will provide appropriate notice to you, usually through an email message.

Questions or comments?

If you have questions regarding this Workforce Privacy Policy, please call to speak to one of our HR professionals at 281-776-7000.

You can also send a written inquiry to:

Tailored Brands
Corporate Relations
6380 Rogerdale Rd
Houston, Texas 77072

Effective Date: May 4, 2020

Last Revised: December 21, 2022