# Privacy Notice for California Employees and Job Applicants

COMPANY Thrift Management Company, LLP, Valley Thrift Store, LLC and Community Thrift Store, LLC are committed to protecting your privacy. The information that you provide to us (sometimes referred to as "we", "us", "our", or "COMPANY") is utilized in order for us to (among other things) consider you for employment, retain you as an employee and to maintain employment records.

This Notice to California Employees and Job Applicants ("Notice") applies to our offline and online data collection practices, including when you submit personal data for purposes of applying for and/or becoming a valued employee at COMPANY, and in the course of your employment with COMPANY, pursuant to California law, including the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA"). If you are not an employee or job applicant who is a California resident, this Notice does not apply to you.

**Your Consent**

Please review this Notice periodically. You should read this entire Notice before submitting information, including personal information, to us in any form. Whenever you submit personal information to us, you consent to the collection, use, disclosure, transfer, and storage of that information in accordance with this Notice.

All personal information may be used for the purposes stated in this Notice. We may make full use of all information that is de-identified, aggregated, or otherwise not in personally identifiable form.

**COLLECTION OF PERSONAL INFORMATION**

We collect personal information from you when you choose to voluntarily provide it for purposes of employment with COMPANY or applying for employment with COMPANY. We collect Personal Information such as your name, job title, mailing address, right to work for I-9 verification, phone number, date of birth, gender, names and relationships of dependents, emergency contact information, credit check, background check, resume with professional, employment and educational background, language proficiency, beneficiary designations, garnishment notices from tax agencies, proof of identification, doctor's notes, diversity and EEO data collection.

We collect Sensitive Personal Information such as personal identification numbers, including social security, driver's license, passport, or state ID card numbers; banking information; diversity and EEO data collection including race and ethnicity, sexual orientation, military and disability status.

We collect information about you through your browser, computer hardware and software. (This information can include your IP address, device ID, browser type, domain names, access times and dates, pages viewed, one or more cookies that may uniquely identify your browser, referring website addresses, what applications are run on your company issued device, files downloaded, opened, and created using company managed equipment, geolocation of laptops and mobile devices which contain company data, and any personal information entered into any company controlled system, including company email.)

To see a complete list of what we collect, how we use this data, please see our **Annex 1**.

**HOW WE USE YOUR EMPLOYEE PERSONAL INFORMATION**

We use Personal Information of employees and job applicants for a wide range of purposes, including:

- to evaluate job candidacy and communicate with you regarding your application;
- to keep you up-to-date about the employment process and employment-related issues;
- to ensure compliance with internal HR policies;

- to facilitate the employment relationship, including for processing of payroll and benefits (including family health benefits), and other internal business needs;
- to maintain internal employment records;
- to maintain internal financial records including paystubs and payment methods;
- to meet and monitor government reporting regulations;
- to comply with legal obligations or to assert or defend legal rights or address legal claims and proceedings; and,
- to maintain any other business operations.

**HOW WE DISCLOSE YOUR EMPLOYEE PERSONAL INFORMATION**

**Service Providers and Contractors**

We disclose Personal Information you provide to consultants, service providers, and contractors that we use to support our business and operations who have agreed to keep the information confidential and use it only to provide the applicable service(s) such as vendors that help us communicate with you, vendors that host our website and data, security and fraud detection vendors.

**Legal Obligations**

We may disclose Personal Information to outside parties (including, without limitation, governmental agencies) if required to do so by law, regulation or court order; to respond to governmental and/or law enforcement requests; to identify, contact or bring legal action against someone who may be causing injury to or interfering with our (or others') rights or property; to support any actual or threatened claim, defense or declaration in a case or before any jurisdictional and/or administrative authority, arbitration or mediation panel; or in connection with disciplinary actions/investigations.

**Sale or Corporate Restructuring**

We may disclose Personal Information to non-parties in connection with the sale, assignment or other transfer of the business of our website or the sale, assignment, merger, reorganization or other transfer of our brand or company.

To see a complete list of what we collect and how we use and disclose that information, please see our **Annex 1**.

**RIGHTS UNDER THE CCPA AND CPRA**

Under California law, as an employee, you are afforded several rights, as discussed further below, about the personal information collected about you. However, there are several exceptions that may apply. These exceptions to the right to request to access, correct, amend, and/or delete your personal information may include our right to maintain personal information of employees for business purposes and solely internal uses reasonably aligned with the expectations of the employee, as well as to comply with any legal obligations, including maintaining proper employee records, or maintaining privilege or confidentiality of certain records, in compliance with applicable U.S. and California labor laws and legal rights.

**RIGHT TO KNOW ABOUT PERSONAL INFORMATION COLLECTED OR DISCLOSED**

**Personal Information Collected**

In the past 12 months, we have collected the categories of personal information about California employees and job applicants as described in Annex 1 to this Notice.

**Information Sold or Shared**

We have not sold or shared personal information about California employees or job applicants in the past 12 months.

We have disclosed the following categories of personal information about California employees and job applicants for a business or commercial purpose in the preceding 12 months:

- IP address, device ID, browser type, domain names, access times and dates, pages viewed, one or more cookies that may uniquely identify your browser, referring website addresses, what applications are run on your company issued device, files downloaded, opened, and created using company managed equipment, geolocation of laptops and mobile devices which contain company data, and any personal information entered into any company controlled system, including company email.
- Name, job title, mailing address, right to work for I-9 verification, phone number, date of birth, gender, names and relationships of dependents, emergency contact information, credit check, background check, resume with professional, employment and educational background, language proficiency, beneficiary designations, garnishment notices from tax agencies, proof of identification, health information, diversity information and EEO data collection.

**Requests to Know**

You have the right to request that we disclose personal information we collect about you.

To make a request for any of the information set forth above (a "Request to Know"), please submit a verifiable employee request pursuant to the instructions below. You may only make a Request to Know twice within a 12-month period. We will acknowledge your Request to Know within 10 days and will attempt to respond substantively within 45-90 days.

The Request to Know must provide sufficient information to allow us to verify that you are the person about whom the personal information was collected or disclosed and must contain sufficient detail to allow us to properly understand, evaluate and respond to your request. If we cannot verify your identity, we will not be able to respond to your request.

You can make a Request to Know the personal information we have about you by using our **Webform** or calling **1 (800) 775-8387.**

Once we receive your Request to Know, we will begin the process to verify that you are the person that is the subject of the request (the "Verification Process"). The Verification Process consists of matching identifying information provided by you with the information we have about you in our records.

**RIGHT TO KNOW SENSITIVE PERSONAL INFORMATION COLLECTED**

We collect and use your Sensitive Personal Information as described in **Annex 1**. We do not collect or process sensitive personal information for the purpose of inferring characteristics or for any purpose other than those set forth in CPRA Regulations, Article 3, Section 7027(m).

**RIGHT TO REQUEST DELETION OF PERSONAL INFORMATION**

You have the right to request the deletion of your personal information collected or maintained by us ("Request to Delete"), subject to certain exceptions permitted by law.

To make a Request to Delete, please submit a verifiable employee request pursuant to the instructions below. We will acknowledge your Request to Delete within 10 days and will attempt to respond substantively within 45-90 days.

The Request to Delete must provide sufficient information to allow us to verify that you are the person about whom the personal information was collected, sold or disclosed and must contain sufficient detail to allow us to properly

understand, evaluate and respond to your request. If we cannot verify your identity, we will not be able to respond to your request. Additionally, as permitted by law, if the information requested to be deleted is necessary for us to maintain, we will not be able to comply with your request. We will notify you if this is the case.

You can make a Request to Delete by using our **Webform** or calling **1 (800) 775-8387.**

Once we receive your initial request to delete and your separate confirmation to delete, we will need to verify that you are the person that is the subject of the request (the "Verification Process"). The Verification Process consists of matching identifying information provided by you with the information we have about you in our records.

We will retain correspondence, documents and information related to any Request to Know, Request to Delete, or Request to Opt-Out for 24 months as required by law.

**RIGHT TO CORRECT**

You have the right to request that we rectify inaccurate information about you.

**Requests to Correct**

To make a Request to Correct, please submit a verifiable employee request pursuant to the instructions below. We will acknowledge your Request to Correct within 10 business days and we will attempt to respond substantively within 45-90 days.

You can make a Request to Correct by using our **Webform** or calling **1 (800) 775-8387.**

Once we receive your request to correct, we will need to verify that you are the person that is the subject of the request through the Verification Process.

We will review all information provided by you to us, to determine whether the information is inaccurate. We reserve the right to delete the information instead of correcting if such deletion does not impact you or you consent to the deletion.

We will inform you of our decision to deny or grant your request.

We will retain correspondence, documents and information related to any Request to Correct for 24 months as required by law.

**RIGHT TO NON-DISCRIMINATION FOR EXERCISING CONSUMER PRIVACY RIGHTS**

You have the right not to receive discriminatory treatment for exercising your privacy rights conferred by the California Consumer Privacy Act, including by exercising the rights specified herein.

**RETENTION OF PERSONAL INFORMATION**

We will retain your Personal Information for as long as it is necessary for the purposes set out in **Annex 1** and to the extent necessary to comply with our legal obligations (for example, if we are required to retain your Personal Information to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

**AUTHORIZED AGENT INFORMATION**

You may designate an authorized agent to make a request on your behalf under the California Consumer Privacy Act.

In order to allow an authorized agent to make a request on your behalf, by using our **Webform** or calling **1 (800) 775-8387.**

When your authorized agent makes a request related to your personal information, we will require the agent to provide the above written permission. We may also require that you verify your own identity directly with us at the time such a request is made.

**Changes to This Employee Notice**

This Employee Notice may be revised from time to time for any reason. If this Employee Notice changes, the revised Notice will include a new effective date, and we will notify you of such changes by posting the revised policy on this page. Be sure to check the Notice whenever you submit personal information to us.

**GOVERNING LAW**

This Notice along with our privacy practices will be subject exclusively to the laws of the State of California, United States of America. We make no representation that this Notice and its practices comply with the laws of other jurisdictions.

**CONTACT FOR MORE INFORMATION**

For information and questions about the use of your personal information or this Employee Notice or your rights under California law, you may contact Human Resources at hr@mmthrift.com.

**ANNEX 1**

**Notice of Collection, Use, and Disclosure**

| Category | Examples | Collected From | Purposes | Disclosed to | Sold or Shared | Retention Period |
|---|---|---|---|---|---|---|
| **Personal Identifiers** | Name, job title, mailing address, right to work for I-9 verification, phone number, date of birth, gender, names and relationships of dependents, emergency contact information, credit check, background check, resume with professional, | You when you apply for an employee position and when you join our company as an employee. | To evaluate job candidacy and communicate with you regarding your application;<br>To maintain internal business employment records;<br>To authenticate your account credentials and identify | Consultants, service providers, and contractors that we use to support our business and operations (e.g. processing payments to employees, and providing fraud detection services) who have agreed to keep the information confidential and use it only | No | We will retain your Personal Information for as long as it is necessary and to the extent necessary to comply with our legal obligations, resolve disputes, and enforce our legal agreement |

| Category | Examples | Collected From | Purposes | Disclosed to | Sold or Shared | Retention Period |
|---|---|---|---|---|---|---|
| | employment and educational background, language proficiency, beneficiary designations, garnishment notices from tax agencies, proof of identification, doctor's notes, diversity and EEO data collection. | | you, as necessary to log you in and/or ensure the security of your account; and<br><br>To comply with our policies, procedures, and legal obligations, including complying with law enforcement or governmental authority requests, investigating fraudulent activity, resolving disputes, and enforcing our legal agreements and policies. | to provide the applicable services;<br><br>Other parties (including, without limitation, governmental agencies) if required to do so by law, regulation or court order; to respond to governmental and/or law enforcement requests;<br><br>An acquirer or successor-in-interest in the event of a reorganization, merger, sale, change of control, consolidation, joint venture, assignment, transfer or other disposition of all or any part of COMPANY or its affiliates including any negotiation thereof. | | s and policies. |

| Category | Examples | Collected From | Purposes | Disclosed to | Sold or Shared | Retention Period |
|---|---|---|---|---|---|---|
| **Financial Information** | Banking Information | You when you are hired. | To process payroll.<br><br>To comply with our policies, procedures, and legal obligations, including complying with law enforcement or governmental authority requests, investigating fraudulent activity, resolving disputes, and enforcing our legal agreements and policies. | Consultants, service providers, and contractors that we use to support our business and operations (e.g. processing payments to employees, and providing fraud detection services) who have agreed to keep the information confidential and use it only to provide the applicable services;<br><br>Other parties (including, without limitation, governmental agencies) if required to do so by law, regulation or court order; to respond to governmental and/or law enforcement requests;<br><br>An acquirer or successor-in-interest in the | No | We will retain your Personal Information for as long as it is necessary and to the extent necessary to comply with our legal obligations, resolve disputes, and enforce our legal agreements and policies. |

| Category | Examples | Collected From | Purposes | Disclosed to | Sold or Shared | Retention Period |
|---|---|---|---|---|---|---|
| | | | | event of a reorganization, merger, sale, change of control, consolidation, joint venture, assignment, transfer or other disposition of all or any part of COMPANY or its affiliates including any negotiation thereof. | | |
| **Biometric Information** | Fingerprint Data. | You when you join our company as an employee. | To verify identity for timeclocks. | Consultants, service providers, and contractors that we use to support our business and operations (e.g. payroll timekeeping services, processing payments to employees, and providing fraud detection services) who have agreed to keep the information confidential and use it only to provide the | No | We will retain your Personal Information for as long as it is necessary and to the extent necessary to comply with our legal obligations, resolve disputes, and enforce our legal agreements and policies. |

| Category | Examples | Collected From | Purposes | Disclosed to | Sold or Shared | Retention Period |
|---|---|---|---|---|---|---|
| | | | | applicable services;<br><br>Other parties (including, without limitation, governmental agencies) if required to do so by law, regulation or court order; to respond to governmental and/or law enforcement requests. | | |
| **Sensitive Personal Information** | Personal identification numbers, including social security, driver's license, passport, or state ID card numbers; banking information; diversity and EEO data collection including race and ethnicity, sexual orientation, military and | You when you apply for an employee position and when you join our company as an employee. | To maintain internal business employment records;<br><br>To authenticate your account credentials and identify you, as necessary to log you in and/or ensure the security of your account; and<br><br>To comply with our policies, procedures, and legal obligations, | Consultants, service providers, and contractors that we use to support our business and operations (e.g. processing payments to employees, and providing fraud detection services) who have agreed to keep the information confidential and use it only to provide the | No | We will retain your Personal Information for as long as it is necessary and to the extent necessary to comply with our legal obligations, resolve disputes, and enforce our legal agreements and policies. |

| Category | Examples | Collected From | Purposes | Disclosed to | Sold or Shared | Retention Period |
|---|---|---|---|---|---|---|
| | disability status. | | including complying with law enforcement or governmental authority requests, investigating fraudulent activity, resolving disputes, and enforcing our legal agreements and policies. | applicable services;<br>Other parties (including, without limitation, governmental agencies) if required to do so by law, regulation or court order; to respond to governmental and/or law enforcement requests. | | |
| **Health** | Doctor's notes. | You when applying for medical leave;<br>You when requesting sick leave pay;<br>You when you give authorization to your doctor's office to provide us with medical paperwork to process any medically related work claims. | To process health related claims. | Consultants, service providers, and contractors that we use to support our business and operations (e.g. processing payments to employees, and providing fraud detection services) who have agreed to keep the information confidential and use it only to provide the | No | We will retain your Personal Information for as long as it is necessary and to the extent necessary to comply with our legal obligations, resolve disputes, and enforce our legal agreements and policies. |

| Category | Examples | Collected From | Purposes | Disclosed to | Sold or Shared | Retention Period |
|---|---|---|---|---|---|---|
| | | | | applicable services;<br><br>Other parties (including, without limitation, governmental agencies) if required to do so by law, regulation or court order; to respond to governmental and/or law enforcement requests. | | |
| **Internet/ Network/ IT Information** | IP address, device ID, browser type, domain names, access times and dates, pages viewed, one or more cookies that may uniquely identify your browser, referring website addresses, what applications are run on your company issued device, files | You, upon issue and use of COMPANY devices. | To maintain IT services;<br><br>To store backups of information on employee devices;<br><br>To authenticate your account credentials and identify you, as necessary to log you in and/or ensure the security of your account; and<br><br>To comply with our policies, | Consultants, service providers, and contractors that we use to support our business and operations (e.g. processing payments to employees, and providing fraud detection services) who have agreed to keep the information confidential and use it only to provide the | No | We will retain your Personal Information for as long as it is necessary and to the extent necessary to comply with our legal obligations, resolve disputes, and enforce our legal agreements and policies. |

| Category | Examples | Collected From | Purposes | Disclosed to | Sold or Shared | Retention Period |
|---|---|---|---|---|---|---|
| | downloaded, opened, and created using company managed equipment, geolocation of laptops and mobile devices which contain company data, and any personal information entered into any company controlled system, including company email. | | procedures, and legal obligations, including complying with law enforcement or governmental authority requests, investigating fraudulent activity, resolving disputes, and enforcing our legal agreements and policies. | applicable services;<br>Other parties (including, without limitation, governmental agencies) if required to do so by law, regulation or court order; to respond to governmental and/or law enforcement requests. | | |

Updated February 2024