

TrellisWare Employee and Applicant Privacy Notice

Last updated: March 12, 2026

This TrellisWare Employee and Applicant Privacy Notice (“**Notice**”) applies to all job applicants, current and former employees, owners, directors, officers, and contractors who work for or on behalf of TrellisWare Technologies, Inc. and any subsidiary, affiliate, or branch that we have or may subsequently form (“**TrellisWare**”). We adopt this Notice to comply with the California Consumer Privacy Act of 2018 (CCPA), as revised by the California Privacy Rights Act of 2023 (CPRA) and its implementing regulations, and other applicable U.S. state laws. Any terms defined in the CCPA have the same meaning when used in this Notice. During your work with or for TrellisWare we may need to collect, use, and store information that is personal to you. We are committed to protecting the privacy and security of such personal information and to being transparent about the purposes for which we use your personal information. This Notice sets forth our policies and practices for handling the information we collect and use in the employment context.

EU/UK Residents: If you reside in the European Union or the United Kingdom, the EU/UK Addendum to this Notice applies to you and supplements and modifies this Notice as set forth in that Addendum. In the event of any conflict between this Notice and the EU/UK Addendum, the EU/UK Addendum will control with respect to individuals residing in the European Union or United Kingdom.

Categories of Personal Information We Collect and How We Use It

TrellisWare collects and processes information from you for human resource, employment, and benefit administration purposes, to otherwise accomplish our business purposes and objectives (including, for example, administration of security clearances; conducting research, analytics and data analysis, maintaining our facilities and infrastructure, quality and safety assurance measures, conducting risk and security controls and monitoring, detecting and preventing fraud, performing identity verification, and to conduct internal investigations), and where necessary to comply with any local, state, and federal legal obligations, internal policies, and contractual obligations. We obtain the categories of personal information listed below directly from you and the information you provide during your job application process, with our clients, or with our recruiters, your employee onboarding process, and during the selection of your benefits as an employee. In some cases, we may obtain a background check and/or consumer report from a consumer reporting agency once an offer of employment is made.

We collect personal information for employment and contractual purposes, including the following:

- **Identifiers:** Name, alias and other names, email address, telephone or mobile number, and address.
- **Protected Classification Characteristics:** Age, veteran or military status, education, marital status, and disability status.
- **Employment Information:** Job title, department, employment status, work history, performance reviews, compensation, benefits, and leave data.
- **Health Information:** Benefits-related health data (e.g., medical leave and insurance enrollment).
- **IT and Usage Data:** IP address, sign-in and device information (including username and password), account name or number, and other online or device identifiers.

We may also collect sensitive personal information for employment or contractual purposes, including the following:

- **Government Identifiers:** Social Security Number, driver's license number or state ID card number, passport number
- **Identity and Demographics:** Racial or ethnic origin, citizenship or immigration status, religious beliefs, philosophical beliefs, union membership, and sexual orientation (including gender, gender identity, or gender expression).
- **Financial Information:** Bank account details for payroll and direct deposit, debit card number, credit card number, tax selections, and any reimbursement requests.
- **Health and Biometric Data:** Health information, genetic data, and biometric information (e.g., fingerprints) used for secure and badge access, unique identification, and time/ attendance services.
- **Location:** Precise geolocation.

We only retain personal information about you for as long as necessary to fulfill the purposes we collected it for or as required to satisfy any legal, accounting, contractual, reporting, or record retention obligations. Retention periods may vary by category.

Disclosure of Personal Information to Third Parties

TrellisWare does not sell or otherwise disclose your personal information to any third parties for any monetary consideration. We may disclose your personal information to the following categories of recipients: (1) TrellisWare affiliates; (2) external service providers; (3) governmental, regulatory, and supervisory authorities, and/or judicial agencies, as permitted or required under applicable law; (4) potential investors and their advisors, auditors and legal counsel in connection with a corporate restructuring, sale, merger, or other changes of control; and (5) to third parties in circumstances where we are required to do so by law, regulation, or legal process. We may also disclose your citizenship and/or US Person status to governmental and commercial entities that we contract with to the extent necessary to demonstrate compliance with related contractual restrictions.

Protection of Personal Information & Your Rights

This Notice is intended to comply with applicable U.S. state privacy laws, including the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). Although certain rights described below are derived from California law, TrellisWare provides these rights to all employees and applicants, except as otherwise specified in this Notice or in any applicable jurisdiction-specific addendum. Subject to applicable exceptions and verification requirements, you have the following rights with respect to personal information we have collected about you in the employment context:

Right to Know/Access: You have the right to request certain information about our collection and use of personal information about you as described below:

- The specific pieces of your personal information collected.
- The categories of your personal information collected.
- The categories of sources from whom your personal information is collected.
- The purpose for collecting your personal information.
- The categories of third parties with whom we have shared your personal information.

Right to Data Portability: You may request a copy of your personal data in a portable and a non-accessible format.

Right to Delete: You have the right to request that we delete certain personal information we have about you.

Freedom from Discrimination: You have the right to be free from unlawful discrimination for exercising any of the rights above.

Right to Correct: You have the right to request that we correct inaccurate personal information regarding the information you provide us.

Right to Restrict the Use of Sensitive Personal Information (U.S. Residents Only): You have the right to restrict the use of your sensitive personal information.

Right to Access Information on Automated Decision-Making: You have the right to access information collected through automated decision-making. Additionally, you can opt-out of our use of automated decision-making related to your personal information.

To make a request in relation to the above rights, please contact us using the contact information below. To fulfill your request, we will need to verify your identity. Only you or someone legally authorized to act on your behalf may make a request related to your personal information. To designate an authorized agent, the authorized agent must provide sufficient information that allows us to reasonably verify that you authorize them to act on your behalf.

Data Security

We implement commercially reasonable physical, technical, and administrative safeguards designed to protect your personal information. Access to personal data is restricted to authorized personnel only and is stored securely. Security measures include encryption, access controls, and monitoring of network and device activity designed to prevent unauthorized access.

Contact Information & Updates

We may update this Notice from time to time, in which case the revised notice will be posted to our intranet or provided to you in writing, by email, or mail. If you have any questions about this Notice and the ways in which we collect and use your information, please do not hesitate to contact us through the privacy officer (Legal Dept.) at legal@trellisware.com or at:

TrellisWare Technologies, Inc.
Attn: TrellisWare Privacy Office (Legal Department)
10641 Scripps Summit Court, Suite 100
San Diego, CA 92131

EU/UK Addendum to Employee and Applicant Privacy Notice

This European Union and United Kingdom Addendum (“EU/UK Addendum”) supplements and modifies the TrellisWare Employee and Applicant Privacy Notice (the “Notice”) and applies solely to job applicants, current and former employees, owners, directors, officers, and contractors who work for or on behalf of TrellisWare Technologies, Inc., and any subsidiary, affiliate, or branch that we have or may subsequently form (“**TrellisWare**”), and who reside in or are located in the European Union or the United Kingdom.

This EU/UK Addendum is intended to comply with the General Data Protection Regulation (Regulation (EU) 2016/679) (“GDPR”), the UK General Data Protection Regulation (“UK GDPR”), and applicable data protection laws of the European Union Member States and the United Kingdom.

In the event of any conflict between the Notice and this EU/UK Addendum, this EU/UK Addendum will control with respect to individuals to whom it applies.

Except as expressly modified by this EU/UK Addendum, the Notice remains in full force and effect.

Legal Bases for Processing

Under the GDPR, we rely on the following legal bases for processing your personal data:

- To perform our contractual relationship, including managing employment or contractor relationships.
- To fulfill our legal obligations with respect to payroll, tax, immigration, health and safety, and reporting obligations.
- Because it is in our legitimate interest to run an effective and efficient business through, among other things, conducting access control and security monitoring, fraud prevention, business planning and analytics, and IT security and network monitoring.
- Because you have provided your consent for us to do so.

Where we process sensitive personal data, which includes (i) information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; (ii) genetic and biometric data, and (iii) data concerning health, sex life, or sexual orientation, we process information either (i) because we have your consent to do so or (ii) because we are required to process the information to comply with applicable laws.

When we process your sensitive personal data on the basis of your consent, you may withdraw that consent at any time by contacting legal@trellisware.com. If you withdraw your consent, we may still be required to process your Sensitive Personal Information to comply with applicable law, but we will explain to you at the time your consent is withdrawn what processing activities will continue for legal compliance purposes.

International Data Transfer

TrellisWare is a global company. We transfer your data to the United States, the Netherlands, and the other countries where we operate. If you apply for employment at one of our E.U. or U.K. sites, your data will be accessed by our headquarters in the United States and the applicable E.U. or U.K. site as appropriate to evaluate your employment application.

Data Retention

Except as otherwise permitted or required by applicable law or regulation, we will only retain your personal data for as long as necessary to fulfill the purposes we collected it for, as required to satisfy any legal,

accounting, or reporting requirements, or as necessary to resolve disputes. To determine the appropriate retention period for personal data, we consider our statutory obligations, the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes we process your personal data for, and whether we can achieve those purposes through other means.

We specify the retention periods for your personal data in our data retention policy. Under some circumstances we may anonymize your personal data so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent. If you are offered and accept employment with us, the personal data we collected during the application and recruitment process will become part of your employment record, and we may use it in connection with your employment consistent with our employee personal data policies. If you do not become an employee, or, once you are no longer an employee, we will retain and securely destroy your personal data in accordance with our document retention policy and applicable laws and regulations.

Your Rights

In addition to the rights described in the Notice, where the GDPR or related data protection laws apply, the following rights may be available to you:

Access: You have the right to access personal data we hold about you, how we use it, and who we share it with.

Correction: You have the right to correct any personal information held about you that is inaccurate and have incomplete data completed.

Erase: You have the right to request we erase the personal information we hold about you in certain circumstances (e.g.; it is no longer necessary for us to hold that information; you have withdrawn your consent; we are processing the personal information on the basis of our legitimate interest and you object to such processing; or you believe your personal information is being unlawfully processed by us). We will retain the personal data if there are valid grounds under law for us to do so (e.g., for the defense of legal claims or freedom of expression).

Restriction of processing to storage only: In certain circumstances, you have the right to require us to stop processing the personal information we hold about you other than for storage purposes (e.g., for a period of time to determine the accuracy of your personal information or when exercising your right to object; or if you require us to retain the personal information for certain purposes such as the defense of legal claims). If we stop processing the personal data, we may use it again if there are valid grounds under law for us to do so.

Objection: In certain circumstances, you have the right to restrict or object to our processing of your personal information. We may continue to process your personal data if there are valid grounds under law for us to do so (e.g., compelling legitimate grounds or for the defense of legal claims).