



Employee Privacy Notice

Date: 2/1/2026

Revision: 1.0

NOTICE TO READERS

This document is published by Digital Trusted Identity Services (DTIS) for transparency and informational purposes. While the content reflects DTIS's current practices and commitments, it may be updated periodically to reflect legal or operational changes. No part of this document may be reproduced, modified, or distributed for commercial purposes without prior written permission from DTIS.

© Digital Trusted Identity Services 2026


All Rights Reserved

Public Information

Revision History

Rev. #	Date	Author	Description
1.0	2/1/2026	Mark Sward	Initial Version

Approval

Name	Title	Role	Signature	Date
Eric Lapp	Chief Executive Officer	Policy Owner	 <small>Eric Lapp (Mar 5, 2026 14:48:34 EST)</small>	Mar 5, 2026

Review Schedule

This Employee Privacy Notice is reviewed at least annually or upon any material changes to our data processing practices, applicable laws, or business operations.

Next scheduled review date: *February 1, 2027*

Table of Contents

Revision History	2
Approval	2
Review Schedule	2
Table of Contents	3
Purpose	4
Important information	4
How can you contact DTIS about privacy?	4
How might DTIS change its privacy notices?	4
What happens if you do not provide your personal data?	5
What data will DTIS collect?	5
How does DTIS collect your data?	6
Once collected, how does DTIS use personal data?	6
Does DTIS sell, share or disclose personal data to third parties?	8
Personal Information Disclosure: United States or Overseas	9
How long is personal data retained for?	9
What happens if there is a change in the purpose of processing?	9
Does DTIS provide links to third party websites?	9
What are your rights?	10
What rights do you have in California?	10
What rights do you have under other state consumer privacy laws (other than California)?	10
How do you exercise your rights under state privacy laws in the United States (including California)?	12

Purpose

Digital Trusted Identity Services (“DTIS”, “we” or “us”) is committed to protecting your privacy. This privacy notice applies to actual and prospective employees or contractors of DTIS in the United States. Throughout this notice, we may use the terms “employee”/ “employment” or “candidate”/ “candidacy”. In all cases this is intended to refer to both employees and contractors.

For information on our privacy practices related to marketing, sales, and general use of our website, please see our website privacy policy [here](#). For more detailed information on our privacy practices when performing identity and background check services, please see our Services Privacy Notice [\[link\]](#).

Important information

This privacy notice tells you how DTIS collects and processes personal data about you in connection with your application for employment or employment, including in processing a background check about you for employment purposes in accordance with DTIS’s screening policies and procedures. Some positions with DTIS may require screening through a government entity, which may include (but is not limited to) obtaining a national security clearance or special license. In those cases, DTIS does not control the screening requirements, the personal information that must be collected, or how that information is processed or otherwise handled. Where this applies to you, you should receive a separate privacy notice.

It’s important for you to read this privacy notice along with any other privacy notices we give you when we collect or use your personal information. This way, you’ll understand how and why we use your data. This notice adds to the other notices and does not replace or override them.

DTIS does not employ children. Our websites and systems are not intended for children, and we do not knowingly provide services to or collect data about children. We do not knowingly collect, sell, or share personal information of consumers under the age of 16.

If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact us using the details set out below.

How can you contact DTIS about privacy?

- **Questions about a background check**
 - If you have a question about a background check DTIS conducted about you when you were a candidate or employee of DTIS, please
- **Report Requests and Disputes**
 - If you would like to (a) request a copy of any background report(s) DTIS prepared about you or the information in our files (if any) about you, or (b) dispute the accuracy of the information in your background report, please contact your Recruiter or Human Resources Representative.
- **Privacy Notice questions**
 - If you have any questions specifically regarding our privacy policy, you may contact us by submitting a request to Human Resources (HR) (if you are a current employee) or emailing privacy@dtis.com (if you are a candidate). You may also contact us at 10201 Fairfax Boulevard, Suite 470, Fairfax, Virginia 22030. In accordance with California Civil Code § 1786.20, these representatives will be able to assist you with additional information regarding our privacy practices and policies.

How might DTIS change its privacy notices?

DTIS may revise the policies that this Privacy Notice describes from time to time. If there is a material change to the policies that this Privacy Notice describes, we will post the revised notice at this location. Except as required by law, we will not use your information for new purposes that are not described in this notice without first making a reasonable

attempt to notify you. We encourage you to periodically review this Privacy Notice to be informed of how DTIS is collecting, processing, and protecting your information.

What happens if you do not provide your personal data?

When we need to collect personal data to fulfill your background check, manage benefits programs or payroll, maintain employee records, or any other task related to your candidacy or employment and you do not provide that personal data, we may be unable to carry out that task. To understand the potential impact of this, please contact your Recruiter or HR Representative with the specific details of your concern.

What data will DTIS collect?

Personal data, or personal information, means any information about an identifiable person. It does not include data that can no longer be associated with an identifiable person (anonymous or anonymized data).

We may collect, use, store and transfer different kinds of personal data about you. We have grouped these kinds of personal data together as follows:

- **Identity Data** includes first name, middle name, last name, previous names, signature, and user name or similar identifier.
- **Contact Data** includes residence and mailing address, delivery address, email address, and telephone numbers.
- **Financial Data** includes bank account details, but not account login information, passwords, or security or access codes that would grant us access to your accounts.
- **Characteristic Data** includes date of birth, age, nationality, race, disability or medical condition, marital or familial status, military or veteran status, sex, and gender.
- **Biometric Data** includes fingerprint information collected for purposes of background checks, employment eligibility verification, or security clearance processing. Fingerprints are captured by authorized third-party agencies and provided to DTIS solely for submission to appropriate governmental authorities. DTIS does not retain fingerprint records after submission, except as required by law.
- **Audio and Visual Data** includes video recordings captured by security cameras located at DTIS facilities for workplace safety and security purposes. Such recordings are stored for a limited period (generally up to 30 days) unless required for investigation or legal purposes. Security cameras are located in common areas of DTIS facilities and are not used to monitor employee productivity.
- **Commercial Data** includes details about your personal property or the products you may obtain from us, for example in connection with an employee recognition program.
- **Geolocation Data** includes information about your location when you are using a company-issued device or interacting with a DTIS webpage, platform, system, or technology.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, internet activity and browsing history, time zone setting and location, browser plug-in types and versions, operating system, platform, and other technology.
- **Profile Data** includes your interests, preferences, characteristics, feedback, survey responses, behavior, attitude, aptitude, and abilities.
- **Usage Data** includes information about how you use our website and systems.
- **Employment Data** includes information about your professional credentials, past employment (including employer names, titles, and dates of employment) and employment with DTIS (including your position and title, your performance history and goal plans, dates of employment, etc.).
- **Education Data** includes information about educational institutions you attended, your name at the time of attendance, and degrees, diplomas, or certificates you earned.

- **Medical Data** includes health insurance data and drug and alcohol testing results.
- **Sensitive personal information** includes certain types of data as part of the following categories:
 - **Identity Data** includes your social security number, driver's license number, passport number, or state identification card information.
 - **Characteristic Data** includes your racial or ethnic origin, citizenship or immigration status.
 - **Technical Data** includes the contents of your emails and text messages, to the extent those communications are sent from or received on a company-issued device.
 - **Geolocation Data** includes precise geolocation data, but only on a company-issued device.

We also collect, use and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data may be derived from personal data about you but is not considered personal data in law, as this data is anonymized and does not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with personal data about you so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

We do not collect, use, or disclose any of the following:

- Genetic information;
- Thermal, olfactory, or similar information; or
- Electronic information except to the extent identified in some category above.

How does DTIS collect your data?

We use different methods to collect data from and about you, including through:

- **Direct interactions.** You may give us your information directly by completing a job application, submitting your resume, entering information in a Workforce Management or Human Resources Information System, supplying information through a background check form, providing information in an interview, or through some other form of direct communication.
- **Automated technologies or interactions.** If you interact with our websites and systems, we may automatically collect information about your equipment, browsing actions, and patterns. When you use a company device, we may monitor, access, and record any activities on the system at any time, subject to applicable laws.
- **Third parties or publicly available sources.** We may receive personal data about you from various third parties and public sources in connection with your application for employment, employment, or a background check we are conducting on you in connection with your employment or application for employment.

Once collected, how does DTIS use personal data?

DTIS may use the personal information you provide to us during the background check process to complete the background screening that is required for the position to which you applied or currently hold. We may also use that personal information in connection with future background screenings. DTIS will provide you with the disclosures required by the FCRA and any other applicable law and obtain your authorization as required by applicable law prior to initiating a background check in most scenarios.

Below, we've included a table that shows all the ways we might use your personal information.

Purpose/Activity	Type of data	Source
To review your application for employment and decide whether or not to hire you	<ul style="list-style-type: none"> • Identity • Characteristic • Contact • Employment • Education • Sensitive personal information 	<ul style="list-style-type: none"> • Direct interactions • Third parties or publicly available sources
To process and deliver payment	<ul style="list-style-type: none"> • Identity • Contact • Financial • Sensitive personal information 	<ul style="list-style-type: none"> • Direct interactions
To process and deliver an order you place through us (e.g. through an employee recognition program)	<ul style="list-style-type: none"> • Contact • Commercial 	<ul style="list-style-type: none"> • Direct interactions
<p>To manage our relationship with you which will include:</p> <ul style="list-style-type: none"> Letting you know about changes to our terms or privacy policy Maintaining and managing employee records Carrying out performance reviews Managing benefits and incentive programs Communicating work- or organization-related updates 	<ul style="list-style-type: none"> • Identity • Contact • Characteristic • Profile • Employment • Medical • Sensitive personal information 	<ul style="list-style-type: none"> • Direct interactions
To let you join a contest or competition or complete a survey	<ul style="list-style-type: none"> • Identity • Contact • Employment • Profile 	<ul style="list-style-type: none"> • Direct interactions
To run and protect our business, systems, and websites (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	<ul style="list-style-type: none"> • Identity • Contact • Employment • Geolocation • Technical • Usage • Sensitive personal information 	<ul style="list-style-type: none"> • Direct interactions • Automated technologies or interactions

Does DTIS sell, share or disclose personal data to third parties?

DTIS does not sell or share employee personal data, as those terms are defined in the California Consumer Privacy Act (CCPA).

- DTIS may disclose personal information to the types of parties set out below as necessary or appropriate in connection with any of the purposes for which we use personal information as described above in “Once collected how does DTIS use personal data?”. Internal parties, meaning [our](#) parent, affiliate, and subsidiary companies or our majority shareholder, HireRight.
- External parties, meaning:
 - DTIS customers. In the course of your role with DTIS, DTIS may disclose your name, business contact information, and title to our customers.
 - Third-party data sources or suppliers. DTIS may disclose your information to certain third parties as necessary to conduct a background check about you in connection with your application for employment or employment.
 - Companies that provide IT and system infrastructure and administration services, which typically act as processors (under some U.S. state privacy law) or as service providers (under California law).
 - Professional advisers (including lawyers, bankers, auditors and insurers) based globally. These companies might provide consultancy, banking, legal, insurance, and accounting services, acting as processors or joint controllers (under some U.S. state privacy law) or as service providers, contractors, or third parties (under California law).
 - Tax authorities, regulators, and other authorities based globally who require reporting of processing activities in certain circumstances, acting as processors or joint controllers (under some U.S. state privacy) or as service providers, contractors, or third parties (under California law).
 - Third-party representatives, service providers, partners, or subcontractors. DTIS may disclose your information to certain third-party representatives or subcontractors authorized by DTIS to assist in carrying out or managing certain tasks related to your application for employment or employment, such as benefit providers.
 - Chatbot or LiveChat providers, such as LivePerson, Cognigy, and Nice inContact.
 - Other parties that we might sell, transfer, or combine parts of our business or our assets with. We might also look to buy other businesses or join together with them. If our business changes hands, the new owners may use your personal information in the same way described in this Privacy Notice.

DTIS transfers to third parties only the personal information that is reasonably necessary for the business purpose for which the information is being provided. DTIS prohibits these third parties from using that information for any other purpose unless they notify you and give you choices about that other purpose. DTIS requires that these parties maintain appropriate measures to protect the confidentiality of your information.

DTIS also may in good faith disclose personal data and any other additional information available to DTIS for any of the following purposes: (i) investigate, prevent or take action regarding actual or suspected illegal activities or fraud, situations involving potential threats to the physical safety of any person, or violations of DTIS's terms of use; (ii) respond to or defend against subpoenas, court orders, or other legal process; (iii) establish or exercise DTIS's legal rights; or (iv) otherwise comply with applicable law.

The table below shows whether, in the 12 months before we published this Privacy Notice, we sold any personal information in the categories listed or disclosed it for business reasons.

“Processors” includes service providers, contractors, and third parties who processes information on our behalf as set out above.

Category	Sold?	Disclosed?
Identity Data	No	Yes, to our processors
Contact Data	No	Yes, to our processors
Financial Data	No	Yes, to our processors
Characteristic Data	No	Yes, to our processors
Commercial Data	No	Yes, to our processors
Geolocation Data	No	Yes, to our processors
Technical Data	No	Yes, to our processors
Profile Data	No	Yes, to our processors
Usage Data	No	Yes, to our processors
Employment Information	No	Yes, to our processors
Education Information	No	Yes, to our processors
Medical Information	No	Yes, to our processors
Sensitive Personal Information	No	Yes, to our processors

Personal Information Disclosure: United States or Overseas

Personal information submitted to DTIS may at times be transferred outside of the United States. All personal information will be transmitted and stored in a secure manner in accordance with the terms of this Privacy Policy.

How long is personal data retained for?

We will keep your personal information only as long as we need it to fulfill the reasons we collected it. This includes meeting any legal, accounting, or reporting requirements.

To decide how long to keep your personal data, we look at several things. These include the amount and nature of personal information, how sensitive it is, the risk of harm if it gets misused, the reasons we process it, whether we can achieve those reasons another way, and any legal or contractual requirements that apply.

What happens if there is a change in the purpose of processing?

We will only use your personal data about you for the purpose(s) we collected it, unless we reasonably think that we need to use it for another reason and that reason is compatible with the original purpose. If this happens and you want to understand how the use for the new purpose is compatible with the original purpose, you can email us at the email address above.

If we need to use your personal information for a different, unrelated reason, we'll let you know and give you a chance to opt-out or ask for your consent if the law requires it.

Keep in mind that we might use your personal information without telling you or asking for your consent first, but we will follow the rules above and do it only if the law requires or allows.

Does DTIS provide links to third party websites?

DTIS may provide links to other websites on our own website, in our systems and trainings, or through other methods. Please remember that we don't control those other sites, and they are not covered by our Privacy Notice. If you have questions about how another site uses your information, check that site's privacy statement.

What are your rights?

In some cases, you have certain rights under data protection laws about your personal information. Below are the specific rights that may apply, depending on where you live.

If you want to exercise any of these rights, please contact us using the information above or in the sections below.

You won't have to pay to access your personal information or to exercise any of your rights. However, we may charge a small fee if your request is clearly unreasonable, repetitive, or excessive, as allowed by law. In some of these cases, we might also refuse your request.

We may need to ask you for specific information to confirm your identity and make sure we're giving your personal information to the right person. This is a safety step to protect your data. We might also reach out for more information to help us respond faster.

We try to answer all valid requests within one month. Sometimes, it might take longer if your request is complicated or if you've made many requests. If that happens, we will let you know and keep you updated.

What rights do you have in California?

If you are a resident of California, you have certain rights related to your personal information under California law. As a California resident, you have the following rights:

- You have the right to ask us to show you the personal information we have collected about you. This includes the categories of information, the categories of sources from which we collected the information, the purpose for collecting, sharing, or selling that information, the categories of third parties with whom we share the information, and the specific pieces of information we have collected.
- If we sell personal information or disclose it for a business purpose, you also have the right to ask for the categories of third parties to whom we sold your information or disclosed your information for a business purpose (by category of personal information in each case).
- You have the right to ask to opt out of our sale or sharing of personal data about you.
- You have the right to ask that we delete any personal information about you that we have collected from you.
- You have the right to ask that we correct any inaccurate personal information we have about you.
- You have the right to limit the use and disclosure of your sensitive personal data.
- You have the right to ask for the specific pieces of personal we have collected about you.
- You have the right to be free of retaliation for exercising your rights under the CCPA.

What rights do you have under other state consumer privacy laws (other than California)?

Many other states in the U.S. have passed consumer privacy laws. However, these privacy laws generally don't apply when to information we process about you or in connection with your employment or application for employment.

If you want to see or correct information we have about you [that](#) falls under this exception, you can still ask for it and we will do our best to assist.

If at any time we collected personal information about you for a purpose unrelated to your application for employment, employment, or background check, you may have the following rights, depending on the state you live in and when the law goes into effect.

Consumer Right	You may have this right starting on the date listed in parenthesis if you live in:
Right to confirm whether we are processing your personal data and access personal data we hold about you	Colorado (1 July, 2023); Connecticut (1 July, 2023); Delaware (1 January, 2025); Indiana (1 January, 2026); Iowa (1 January, 2025); Kentucky (1 January, 2026); Maryland (1 October, 2025); Minnesota (31 July, 2025); Montana (1 October, 2024); Nebraska (1 January, 2025); New Hampshire (1 January, 2025); New Jersey (15 January, 2025); Oregon (1 July, 2024); Rhode Island (1 January, 2026); Tennessee (1 July, 2025); Texas (1 July, 2024); Utah (31 December, 2023); Virginia (1 January, 2023)
Right to request we correct inaccuracies in personal data we hold about you	Colorado (1 July, 2023); Connecticut (1 July, 2023); Delaware (1 January, 2025); Indiana (1 January, 2026); Kentucky (1 January, 2026); Maryland (1 October, 2025); Minnesota (31 July, 2025); Montana (1 October, 2024); Nebraska (1 January, 2025); New Hampshire (1 January, 2025); New Jersey (15 January, 2025); Oregon (1 July, 2024); Rhode Island (1 January, 2026); Tennessee (1 July, 2025); Texas (1 July, 2024); Utah (1 July, 2026); Virginia (1 January, 2023)
Right to request we delete personal data we hold about you	Colorado (1 July, 2023); Connecticut (1 July, 2023); Delaware (1 January, 2025); Indiana (1 January, 2026); Iowa (1 January, 2025); Kentucky (1 January, 2026); Maryland (1 October, 2025); Minnesota (31 July, 2025); Montana (1 October, 2024); Nebraska (1 January, 2025); New Hampshire (1 January, 2025); New Jersey (15 January, 2025); Oregon (1 July, 2024); Rhode Island (1 January, 2026); Tennessee (1 July, 2025); Texas (1 July, 2024); Utah (31 December, 2023); Virginia (1 January, 2023)
Right to obtain a copy of your personal data in a portable and, to the extent technically feasible, readily usable format	Colorado (1 July, 2023); Connecticut (1 July, 2023); Delaware (1 January, 2025); Indiana (1 January, 2026); Iowa (1 January, 2025); Kentucky (1 January, 2026); Maryland (1 October, 2025); Minnesota (31 July, 2025); Montana (1 October, 2024); Nebraska (1 January, 2025); New Hampshire (1 January, 2025); New Jersey (15 January, 2025); Oregon (1 July, 2024); Rhode Island (1 January, 2026); Tennessee (1 July, 2025); Texas (1 July, 2024); Utah (31 December, 2023); Virginia (1 January, 2023)
Right to opt-out of profiling in furtherance of decisions that produce legal or similarly significant effects to you	Colorado (1 July, 2023); Connecticut (1 July, 2023); Delaware (1 January, 2025); Indiana (1 January, 2026); Kentucky (1 January, 2026); Maryland (1 October, 2025); Minnesota (31 July, 2025); Montana (1 October, 2024); Nebraska (1 January, 2025); New Hampshire (1 January, 2025); New Jersey (15 January, 2025); Oregon (1 July, 2024); Rhode Island (1 January, 2026); Tennessee (1 July, 2025); Texas (1 July, 2024); Virginia (1 January, 2023)

Right to opt-out of targeted advertising	Colorado (1 July, 2023); Connecticut (1 July, 2023); Delaware (1 January, 2025); Indiana (1 January, 2026); Kentucky (1 January, 2026); Maryland (1 October, 2025); Minnesota (31 July, 2025); Montana (1 October, 2024); Nebraska (1 January, 2025); New Hampshire (1 January, 2025); New Jersey (15 January, 2025); Oregon (1 July, 2024); Tennessee (1 July, 2025); Rhode Island (1 January, 2026); Texas (1 July, 2024); Utah (31 December, 2023); Virginia (1 January, 2023)
Right to opt-out of sale of personal data we hold about you	Colorado (1 July, 2023); Connecticut (1 July, 2023); Delaware (1 January, 2025); Indiana (1 January, 2026); Iowa (1 January, 2025); Kentucky (1 January, 2026); Maryland (1 October, 2025); Minnesota (31 July, 2025); Montana (1 October, 2024); Nebraska (1 January, 2025); New Hampshire (1 January, 2025); New Jersey (15 January, 2025); Oregon (1 July, 2024); Rhode Island (1 January, 2026); Tennessee (1 July, 2025); Texas (1 July, 2024); Utah (31 December, 2023); Virginia (1 January, 2023)
Right to revoke consent where your consent to our processing of your data was required by law and you provided that consent	Colorado (1 July, 2023); Connecticut (1 July, 2023); Delaware (beginning 1 January, 2025); Maryland (1 October, 2025); Minnesota (31 July, 2025); Montana (1 October, 2024); New Hampshire (1 January, 2025); New Jersey (15 January, 2025); Oregon (1 July, 2024) Rhode Island (1 January, 2026);
Right to appeal a decision we make related to a request to exercise your rights within a reasonable time after that decision	Colorado (1 July, 2023); Connecticut(1 July, 2023); Delaware (beginning 1 January, 2025); Indiana (1 January, 2026); Iowa (1 January, 2025); Maryland (1 October, 2025); Minnesota (31 July, 2025); Montana (1 October, 2024); Nebraska (1 January, 2025); New Hampshire (1 January, 2025); New Jersey (15 January, 2025); Oregon (1 July, 2024); Rhode Island (1 January, 2026);Tennessee (1 July, 2025); Texas (1 July, 2024); Virginia (1 January, 2023)
Right to obtain a list of the specific third parties to which we have disclosed any consumer’s personal data.	Delaware (beginning 1 January, 2025); Minnesota (31 July, 2025); Oregon (1 July, 2024);
Right to obtain a list of the categories of parties to which we have disclosed any consumer’s personal data	Maryland (1 October, 2025)

How do you exercise your rights under state privacy laws in the United States (including California)?

You can make a request to exercise any of your rights under U.S. state privacy laws as described above in the sections What rights do you have in the United States (except California)? and What rights do you have in California? by:

- Emailing us at privacy@dtis.com (if you are a candidate)
- Submitting an HR request (if you are an employee)

If you have already made a request and want to appeal our response, you can do that using the contact methods mentioned above. When you submit your appeal, please make sure to clearly say that you are appealing a previous response.

Employee Privacy Notice



When you submit your request, include your full name, all the email addresses we might have for you, and your employee number.

If you want us to disclose, correct, or delete personal information about you, we may request that you provide a copy of your government-issued ID. Once we review your request, we'll reach out to you with instructions for sending your ID, if we need it.

If you want us to disclose your information to an agent, you need to tell us in writing and give us the mailing address for the agent. If you want an authorized agent to make a request for you, you also need to tell us in writing and include their mailing address.