Services 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.

Revision History

Rev. #	Date	Author	Description
1.0	2/1/2026	Scott Hoenigman	Initial Version

Approval

Name	Title	Role	Signature	Date
Eric Lapp	Chief Executive Officer	Document Owner	Eric Lapp Eric Lapp (Mar 5, 2026 14:48:07 EST)	Mar 5, 2026

Review Schedule

This 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

Purpose

Digital Trusted Identity Services ("DTIS", "we", or "us") is committed to protecting the privacy and security of individuals whose personal information we collect and process. This Privacy Notice describes how we handle and protect personal information while providing identity verification and background check services.

DTIS adheres to the privacy and security principles set forth in the FBI's Criminal Justice Information Services (CJIS) Security Policy and maintains safeguards to ensure the confidentiality, integrity, and availability of personal information. We are committed to processing personal information lawfully, transparently, and in a manner that respects individual rights.

Scope

This Privacy Notice applies to all personal information collected and processed by DTIS while providing identity verification and background check services. It covers information provided by both applicants and customers, regardless of how personal information is collected, whether electronically, through paper forms, or biometric devices.

This notice **does not** apply to any of the following:

- employee data, which is addressed in a separate Employee Privacy Notice;
- data collected for marketing purposes, which is addressed in a separate privacy policy for our website; or
- third-party services or websites that may be linked to from DTIS platforms, which operate under their own privacy policies.

This notice may be supplemented by other, more specific notices, for example our Biometric Privacy Notice which goes into more specific detail about the handling of biometric information.

It's important for you to read this 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.

Definitions

The following terms are used throughout this Privacy Notice:

- **Applicant**: An individual who is the subject of DTIS services (for example, an individual undergoing a fingerprint-based background check).
- **Authorized recipient**: A customer with statutory authority to directly receive and review CHRI from the FBI. DTIS makes CHRI available to these entities through secure systems.
- **Biometric data**: information about the physical, physiological, or behavioral characteristics of an individual, which is both: (a) capable of uniquely identifying the individual; and (b) collected or processed for the purposes of uniquely identifying the individual through automated biometric analysis (e.g., automated comparison of facial or fingerprint geometry). Biometric data includes fingerprint images and fingerprint geometry.
- **Customer**: An organization that uses DTIS services to submit applicants for fingerprint-based background checks. This includes Authorized Recipients as well as organizations that receive CHRI directly from state agencies.
- **CHRI (Criminal History Record Information)**: Information provided by the FBI or state law enforcement agencies that relates to an individual's criminal history.

- **In-Person Enrollment Process**: The in-person enrollment process occurs at the fingerprinting location on the applicant's scheduled date and time. At this stage, an enrollment partner verifies the applicant's identity by reviewing two forms of identification (at least one government-issued photo ID), captures the applicant's fingerprints using an approved device, and securely transmits the biometric and application data to DTIS for further processing.
- **Personal information**: Any information about an identified or identifiable individual.

Data Categories and Collection

DTIS collects different types of personal information to facilitate fingerprint-based background checks and meet regulatory and agency-specific requirements. This data is collected directly from applicants, customers, partners, and authorized government entities.

Biographic Data

Applicants provide personal information through DTIS's secure website. The following fields are collected:

- **Required**: Full name, date of birth, place of birth, U.S. citizen or legal permanent resident status (Y/N), sex, race, height, weight, eye color, hair color, mailing address, and email address.
- **Optional or Conditional**: Aliases, Social Security Number (SSN), Individual Taxpayer Identification Number (ITIN), country of citizenship, employer information, occupation, and data regarding unprintable or amputated fingers.

Contact Data

- Mobile Phone Number
- Email Address

Biometric Data

- **Fingerprint Images**: Captured during in-person enrollment or submitted via fingerprint cards (FD-258) or electronic transmission (EBTS files).
- **Facial Photographs**: Collected when required by government agencies, such as Florida's Agency for Healthcare Administration (AHCA).

For more details about how DTIS handles biometric identifiers and information, please see our Biometric Privacy Notice.

Appointment Data

DTIS collects appointment-related metadata as required to manage appointments and as may otherwise be required by law. Appointment data includes the date and time when an appointment is scheduled, rescheduled, or completed.

Identity Verification Data

As part of the in-person enrollment process, an enrollment partner visually inspects two forms of identification (at least one of which must be a government-issued photo ID) presented by the applicant. This verification step ensures that the person presenting for fingerprinting matches the information submitted online.

Payment Processing Data

To securely process payments for services, DTIS collects credit card information (e.g., card number, expiration date, CVV, name on card).

Technical and Website Usage Data

When users interact with the DTIS website, the following data may be collected automatically:

- IP address
- Browser type and version
- Device information
- Session logs and usage patterns
- Cookies and tracking technologies for session management, analytics, and user experience

CHRI

State and federal agencies, such as the FBI or FDLE, may return system-generated notifications related to submitted transactions, including CHRI.

Purpose of Processing

DTIS collects and processes personal information, including biometric data to facilitate fingerprint-based background checks on behalf of government agencies, authorized recipients, and other eligible organizations. This includes submitting biometric and biographic information to appropriate state and federal entities, such as the FBI and state-level law enforcement.

The table below explains the specific purposes for processing each category of personal information:

Category of Personal information	**Purpose for Processing**
Biographic Data	To identify applicants, verify eligibility, facilitate background check submissions, provide required information to government agencies, communicate with applicants regarding their enrollment, and comply with legal and regulatory obligations.
Contact Data	To create and manage applicant accounts, verify identity where required, communicate regarding scheduling, payments, and background check status, and provide transaction-related notices or updates.
Biometric Data	To capture and process fingerprint images and, where required, facial photographs for submission to authorized government agencies. Biometric data is used solely to support background check processing and compliance with applicable legal and regulatory requirements.
Appointment Data	To schedule and manage fingerprinting appointments, coordinate with enrollment partners, confirm attendance, and provide applicants with reminders or updates related to their enrollment session.
Payment Processing Data	To collect and process service fees, facilitate refunds or adjustments when necessary, maintain transaction

	records for compliance and auditing, and prevent or detect fraudulent activity.
Technical and Website Usage Data	To ensure the security and integrity of our systems, support troubleshooting and performance monitoring, improve user experience on our website, and detect and prevent unauthorized access or fraudulent activity.
Criminal History Record Information	To fulfill authorized background check requests by transmitting CHRI to designated Authorized Recipients or governmental agencies, and to comply with applicable FBI, state, and regulatory requirements.

DTIS is committed to protecting the privacy and security of all personal information and follows applicable privacy regulations and data handling standards, including the CJIS Security Policy. Data is processed only for the purposes described in this notice and is never used for unrelated marketing or other commercial activities.

Data Disclosure

DTIS discloses personal information only as necessary to fulfill our obligations in providing background check services and to comply with legal and regulatory requirements, or for communications with customers. We do not sell or rent personal information. Personal information collected under this notice, other than biometric data or CHRI, may be used for internal marketing or informational purposes directed to our customers, but not for external marketing or advertising to third parties. Biometric data and CHRI are never used for secondary purposes.

Disclosure to Government Agencies

We disclose biographic and biometric data to the following government entities:

- **State and Federal Agencies**: DTIS transmits biographic and biometric data to the FDLE and the FBI for the purpose of conducting fingerprint-based background checks.
- **Florida's AHCA**: When required, we provide facial photographs and appointment metadata related to in-person fingerprint enrollment.

Disclosure to Customers and Authorized Recipients

- **Authorized Recipients**: If a customer is authorized by law to receive CHRI, we make the CHRI available to them for applicants they have submitted.
- **Applicants**: Under FBI Departmental Order 556-73, applicants may receive their own CHRI.
- **Customers**: Our customers, such as employers or agencies that submit individuals for background checks, may view the biographic information of the applicants they submit.

Disclosure to Payment Processors and Financial Institutions

When you make a payment, DTIS collects payment information (e.g., credit card number, expiration date, CVV, and name on card) solely to transmit it securely to our PCI DSS-compliant payment processor.

For client organizations, financial account data (e.g., ACH details) may be securely transmitted to financial institutions to facilitate billing, payment reconciliation, or refunds.

Disclosure to Identity Verification Providers

For FBI Departmental Order 556-73 applicants, DTIS discloses the applicant's contact information to a third-party to verify identity by tying the phone number to their identity in public records before releasing CHRI.

Disclosure to Enrollment Partners

Certain trusted third parties, such as The UPS Store, perform in-person fingerprint enrollments on our behalf. These partners use our secure platform to verify applicant identity and capture fingerprint and photo data where required. Only limited data is presented to them for identity verification purposes.

Legal and Regulatory Disclosures

DTIS may disclose personal information if required by law, including in response to a subpoena or court order. We may also disclose data to regulatory agencies during audits or investigations as required under our contracts with state or federal agencies. The FBI, for example, performs annual compliance audits of our services.

All disclosures are made in accordance with our contractual obligations and our commitment to protecting individual privacy and data security.

The following table describes the way each data type is disclosed, and the recipients or categories of recipients for each data type:

Category of Personal information	**Disclosed?**
Biographic Data	Yes, disclosed to government agencies (e.g., FBI, state agencies, or other authorized recipients) as required to process background checks. Also disclosed to enrollment partners who assist in verifying applicant identity. Not disclosed to any third parties for marketing or unrelated purposes.
Contact Data	Yes, mobile phone numbers (along with certain biographic details) are disclosed to a third-party identity verification provider to support multi-factor authentication and identity resolution. Not disclosed for marketing purposes
Biometric Data	Yes, fingerprint images are disclosed to government agencies to facilitate background checks as part of the channeling process. Facial photographs are disclosed to the State of Florida's AHCA when required for compliance with their program. No biometric data is disclosed for marketing or other secondary purposes.
Appointment Data	Yes, appointment information (e.g., date, time, and location of scheduled fingerprinting) is disclosed to Enrollment Partners to facilitate in-person enrollment. This data is not disclosed externally beyond these purposes.
Payment Processing Data	Yes, payment information (e.g., credit card number, expiration date, CVV, billing name, and ZIP code) is transmitted securely to PCI DSS-compliant third-party payment processors to complete transactions. For client organizations, relevant financial account information (e.g., ACH details) may also be disclosed to financial institutions for billing, refunds, and reconciliation purposes.
Technical and Website Usage Data	No, this data is collected for platform operation, analytics, and user experience purposes. It is not disclosed to third

	parties except in aggregated or anonymized form for reporting or performance monitoring.
Criminal Record History Information	Yes, CHRI is disclosed to authorized recipients and applicants as permitted by law, such as the FBI and state-level agencies. Access is strictly controlled and logged to comply with CJIS and other regulatory requirements.

Data Retention

DTIS retains personal information only as long as necessary to fulfill the purpose for which it was collected, in compliance with FBI requirements and business needs.

CHRI

CHRI is deleted as soon as the authorized recipient or applicant views or downloads it. If it is not accessed, DTIS deletes the CHRI no later than 30 days after receipt, per FBI policy. CHRI is never stored beyond this timeframe. Additionally, each CHRI access is logged with the name of the user, method of access (viewed or downloaded), Transaction Control Number (TCN), and the statutory authority authorizing access. These audit records are retained for period of at least one year.

Biographic Data

Applicants who create an account may have their biographic and contact information retained in the system to support future background checks. Applicants may request deletion of their data at any time, subject to legal or regulatory obligations.

Biometric Data

Fingerprint images and facial photographs are processed and stored in compliance with FBI and state requirements. Data is retained only as long as needed to complete the background check process. CHRI-related biometric data is deleted after the CHRI is delivered or after 30 days, whichever comes first.

Departmental Order Attestation Forms

For applicants submitting a request under FBI Departmental Order 556-73, DTIS retains the signed applicant attestation form for a period of three years or upon termination of the contract, whichever is shorter.

Payment Data

DTIS does not store or retain payment data. Limited billing data (e.g., billing name and ZIP code) may be retained to support receipts, refund processing, and transaction audit trails.

Data Security

DTIS follows the CJIS Security Policy to protect all personal information processed through our systems. We implement multiple layers of protection across data storage, transmission, and access. All data is encrypted both in transit and at rest using industry-standard protocols, including SSL/TLS for transmission. Our databases use Transparent Data Encryption (TDE) to ensure data is encrypted at rest, adding an additional layer of protection. Payment card data is handled in compliance with PCI DSS, securely transmitted directly to a PCI DSS-compliant processor. Access to systems and personal information is strictly limited through role-based access controls, and multi-factor authentication (MFA) is required for Authorized Recipients accessing CHRI. Servers are housed in a secure facility, and all employees undergo

regular security and information security training. DTIS works with carefully selected partners, such as enrollment sites and identity verification providers, who are required to follow secure data handling practices, while data shared with them is limited and accessed only via secure channels. A formal incident response plan is maintained to address potential security events.

Data Subject Rights

DTIS is committed to respecting the rights of individuals whose data we collect and process. Applicants, Authorized Recipients, and Customers may exercise the following rights, depending on the context and applicable laws. While we will consider and respond to any request, we may not be able to fulfill the request in all cases.

- **Right to Access**: The data subject may request a copy of the personal information DTIS holds about them, including the categories of data, sources, processing purposes, and recipients (if any).
- **Right to Rectification**: Individuals may request that DTIS correct inaccurate or incomplete personal information.
- **Right to Erasure (Right to be Forgotten)**: Where applicable, a data subject may request deletion of their personal information. DTIS will honor such requests to the extent permitted by law and contract.
- **Right to Know/Transparency**: Individuals may inquire how their data is processed, why it is collected, and who it is shared with.
- **Right to Withdraw Consent**: Where processing is based on consent, a data subject may withdraw that consent at any time. Withdrawal of consent does not affect processing that occurred prior to withdrawal.
- **Right to Lodge a Complaint**: Data subjects may escalate complaints to a relevant authority or contact DTIS for internal resolution.
- **Right to Opt-Out:** Data subjects may have the right to opt out of certain uses of their personal information, particularly for marketing.
- **Right to Appeal:** Data subjects may have the right to appeal a decision made about a request to exercise their rights.

Submitting Requests

To exercise any of these rights, individuals may contact DTIS using the contact information provided below. We verify the identity of all requestors before fulfilling any rights-based request to protect privacy and ensure compliance.

Children’s Privacy

DTIS does not knowingly collect personal information from children under the age of 13. Our services are intended for use by adults as part of background check and identity verification processes. If we become aware that a child under 13 has submitted personal information through our website or services, we will promptly delete that information.

Changes to This Notice

DTIS may update this Privacy Notice from time to time to reflect changes in legal requirements, our services, or data processing practices. When we make material changes, we will notify users through our website or other appropriate means. We encourage you to review this notice periodically to stay informed about how we protect your information. The “Last Updated” date at the top of this page indicates when this notice was last revised.

Contact Information

If you have questions or concerns about this Privacy Notice or how your data is handled, you may contact us at:

DTIS Privacy Team
10201 Fairfax Blvd #470, Fairfax, VA 22030
Email: privacy@dtis.com
Phone: (703) 797-2562

We take privacy seriously and will respond promptly to your inquiries.