Biometric 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	Policy Owner	Eric Lapp Eric Lapp (Mar 5, 2026 14:43:34 EST)	Mar 5, 2026

Review Schedule

This Biometric 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 biometric data collected in connection with fingerprint-based background checks and identity verification services.

The primary purpose of this notice is to supplement the Services Privacy Notice (available at https://www.dtis.com/privacy/services-privacy-notice.pdf) by explaining how DTIS collects, processes, stores, and protects biometric identifiers in compliance with applicable federal and state laws. Biometric data is collected only to support lawful and authorized background check processing, enrollment verification, and agency-mandated identity confirmation, and it is used solely for these purposes.

DTIS follows the privacy and security principles outlined in the FBI's CJIS Security Policy and maintains safeguards to ensure the confidentiality, integrity, and availability of biometric data. This notice provides transparency to individuals and organizations about our practices and our commitment to handling biometric information responsibly and securely.

Scope

This Biometric Privacy Notice applies to all biometric identifiers and biometric data collected and processed by DTIS in connection with fingerprint-based background checks, identity verification, and enrollment services. It covers biometric data provided by individuals ("applicants") who participate in DTIS services, as well as biometric data submitted by organizations ("customers") or authorized partners for lawful purposes, including employment, licensing, and regulatory compliance.

This document does not apply to other types of personal information or to employee data, which are addressed in separate privacy notices. This notice should be read in conjunction with DTIS's other privacy notices and policies, including the Services Privacy Notice (available at https://www.dtis.com/privacy/services-privacy-notice.pdf) and the Website Privacy Notice (available at https://dtis.com/privacy-policy).

Definitions

The following terms are used throughout this 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, but is not limited to, fingerprint images and fingerprint geometry.
- **CHRI (Criminal History Record Information)**: Information provided by the FBI or state law enforcement agencies that relates to an individual's criminal history.
- **CJIS Security Policy**: The FBI's Criminal Justice Information Services Security Policy that governs the protection of CHRI and other sensitive data.

Purpose of Processing

DTIS collects and processes biometric data to facilitate fingerprint-based background checks on behalf of government agencies, Authorized Recipients, and other eligible organizations.

This data is used exclusively for the following purposes:

- Capturing and processing fingerprints (live-scan and ink-based) and facial photographs for submission to authorized government agencies.
- Ensuring biometric data meets the quality standards required for accurate background checks.
- Supporting the secure and compliant transmission of applicant biometric information in accordance with applicable legal and regulatory requirements.

Biometric data is never used for secondary purposes like marketing or other unrelated commercial purposes.

Data Disclosure

DTIS discloses biometric data only as necessary to fulfill our obligations in providing background check services and to comply with legal and regulatory requirements. We do not sell or rent biometric data.
Biometric data is handled by third parties in the context of DTIS services only as described below:

- **Authorized enrollment partners** capture biometric data during in-person enrollment sessions using DTIS-approved software and hardware. Biometric data is captured on DTIS's behalf and is transmitted directly to DTIS-controlled systems. Enrollment partners do not retain biometric data and do not have independent access to or use of biometric data outside of the enrollment session.
- **State and Federal Government Agencies** (including the FBI, FDLE, and other authorized state agencies) receive biometric data, including fingerprint images, facial photographs (where required), and associated biometric metadata, in EBTS or other approved formats for the purpose of conducting authorized fingerprint-based background checks.

Legal and Regulatory Disclosures

DTIS may disclose biometric data if required by law, including in response to a subpoena or court order. We may also disclose biometric 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.

Data Retention

DTIS retains biometric data only as long as necessary to fulfill the purpose for which it was collected and in compliance with FBI, state, and contractual requirements.

Fingerprint images, facial photographs, and associated biometric metadata are processed and stored solely to complete the background check process. Biometric data related to CHRI is deleted at the earliest of the following:

- When the initial purpose for collection has been satisfied.
- Within thirty (30) days after completion of the background check, unless a longer retention period is required by law or contract.

In any event, biometric data is retained for no more than one year after the purpose for collecting it has expired, or three years after the applicant's last interaction with us, whichever comes first.

Deletion of biometric data is performed through automated processes that remove database records and associated file-based artifacts from active systems. Data is logically deleted from production environments, access references are removed, and stored files are securely deleted. Any remaining copies in backups or replicated systems are retained only in accordance with applicable backup retention and rotation schedules and are not restored or used for operational purposes.

This retention schedule is reviewed at least once per year to ensure compliance with applicable law, and any deletion is carried out in accordance with secure data handling practices.

Data Security

DTIS follows the CJIS Security Policy to protect all biometric data processed through our systems. Biometric data is encrypted both in transit and at rest using industry-standard protocols, and databases employ Transparent Data Encryption (TDE) to ensure data remains secure.

Access to biometric data is strictly limited through role-based access controls, and multi-factor authentication (MFA) is required for Authorized Recipients accessing CHRI. Servers storing biometric data are housed in a secure facility.

A formal incident response plan is maintained to address potential security events affecting biometric data, which includes notifications to affected individuals and third parties in accordance with our legal and contractual obligations.

Changes to This Notice

DTIS may update this 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 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.