FPS Biometric Privacy Policy

Fingerprint Solutions, Inc. (“FPS”, “we” or “us”) collects and processes fingerprints, a type of biometric identifier. This policy explains how we use, disclose, secure, and destroy fingerprints.

Use

We use fingerprints to conduct criminal history record checks with the FBI and state law enforcement agencies (“agencies”). We do not use fingerprints for any other purpose.

Disclosure

We transmit fingerprints to agencies either directly or through third-party channelers that are approved by those agencies.

If a court or law enforcement agency issues a warrant, subpoena, or other enforceable order requiring us to provide your fingerprints, we will do so as required by that order.

Except as described above, FPS never discloses, sells, or shares fingerprints.

Security

FPS follows the FBI’s CJIS Security Policy to protect fingerprints. Fingerprints are encrypted both in transit and at rest using industry-standard protocols, and databases employ Transparent Data Encryption (TDE) to ensure data remains secure.

We strictly limit access to fingerprints through role-based access controls. Servers are located in secure cloud data centers.

We maintain a formal incident response plan to address potential security events affecting your information, which includes notifications to affected individuals and third parties according to our legal and contractual obligations.

Retention and Destruction

We retain fingerprints for 28 days. Once 28 days have passed, we delete your fingerprints through an automatic process that logically deletes them from our database so they can no longer be recovered.