3M Cogent's Privacy Policy

3M Cogent is committed to safeguarding the privacy of applicant's personal information and ensuring the responsible use of the information collected during the fingerprint based background check process. 3M Cogent complies with all state and federal laws for collecting and submitting applicant fingerprint records. The following 3M Cogent Privacy Policy is effective whether data collection takes place over 3M Cogent's secure website, the telephone (Call Center), or at the any of 3M Cogent's fingerprint collection sites.

Collection of Personal Information

In order to submit a fingerprint based background check, applicants are asked to provide demographic data about themselves including critical data elements such as name, date of birth, Social Security Number, and other distinguishing characteristics such as height, weight, sex and race. These are data elements that are required by the specific state and/or federal administrators. Depending on the preferred payment method, credit/debit card information may also be collected. 3M Cogent is in compliance with the Payment Card Industry Data Security Standard (PCI –DSS) when processing, transmitting, or storing applicants' credit/debit card data.

Use of Personal Information

3M Cogent collects and uses applicants' personal information for the sole purpose of generating a state/FBI compliant fingerprint based background check record. 3M Cogent will not disclose applicants' personal information to any entity other than the Authorized Recipient, which is determined by state and federal law. 3M Cogent does not and will not share applicants' personal information with third parties for marketing or other purposes.

3M Cogent fingerprint collection sites and their employees have access to personal applicant information, including fingerprint images and demographic information, which are considered confidential under the law. Applicants' personal data is removed from the fingerprint capture station immediately after the transaction is electronically transmitted to the secure, FBI compliant Applicant Processing Server. 3M Cogent's fingerprint collection sites and their employees are properly trained on the responsible use of applicant information and are required to sign 3M Cogent's Non-Disclosure Form. The responsible use of applicant information is limited to those uses which:

- Are necessary to meet legal and regulatory requirements
- Facilitate positive identification of the applicant prior to fingerprint enrollment.

Security of Personal Information

3M Cogent is compliant with all state/federal laws and industry standards when collecting and transmitting applicant data. 3M Cogent utilizes the latest security technologies to help protect applicants' personal information from unauthorized access, use, or disclosure including:

- Sensitive information is automatically deleted from the fingerprinting (Livescan) machine once the fingerprint data is collected and successfully transmitted.
- 256 bit encrypted transmission.
- Secure Socket Layer (SSL) protocol for Web transmission.
- The backend system removes CHRI immediately after the results are viewed by the Authorized Recipient (or after 30 days, whichever is sooner).
- The computer screen of the Livescan (fingerprint scanner) PC is positioned so that it is out of public view. When the Livescan is not in use, the laptop is closed or the screen is powered off.

3M Cogent, Inc.
5025 Bradenton Avenue, Suite A
Dublin, Ohio 43017 USA

tel. 614.718.9691
fax 614.718.9694
www.cogentsystems.com