Data Retention Policy: Background Checks

Purpose

This data retention policy establishes guidelines for the retention and disposal of Background Check Data by MinistrySafe and Abuse Prevention Systems.

Scope

This policy applies to MinistrySafe and Abuse Prevention Systems regarding Personally Identifiable Information (PII) in Background Check Data, including Background Check Reports, Disclosures and Authorizations.

Retention Periods

MinistrySafe and Abuse Prevention Systems retain Background Check Data for three years, including Background Checks, Disclosures and Authorizations. The retention of these records occurs solely for the purpose of showing member compliance with current standards of care related to sexual abuse risk.

Disposal

Any data identified for disposal is securely deleted or destroyed using methods ensuring the data is not recoverable.

Protection Levels: PII

- All PII must be stored in encrypted files or databases.
- Access to sensitive data is restricted to authorized personnel only, with appropriate access controls and password protection.
- Security audits are conducted regularly to ensure compliance with data protection standards.

Exceptions

Any exceptions to the retention and disposal guidelines delineated in this policy must be approved by the CLO.

Last Updated: 08.22.24 by KDN