# BIOMETRIC DATA RETENTION AND DESTRUCTION POLICY

## SCOPE

This policy applies to all biometric identifiers and biometric information collected, stored, or used by Sedgwick or its authorized vendors in connection with Sedgwick's business operations, including but not limited to:

(a) Pre-employment identity verification processes (e.g., TruePic applicant verification);

(b) Employee identity verification and access control systems;

(c) Any other business process that involves the collection of biometric identifiers or biometric information.

This policy covers biometric identifiers as defined by applicable law, including but not limited to: retina or iris scans, fingerprints, voiceprints, scans of hand or face geometry, and any other biometric data that can be used to identify an individual. Photographs, demographic data, and physical descriptions are excluded to the extent they do not constitute biometric identifiers under applicable law.

## COLLECTION

Sedgwick will not collect, capture, or otherwise obtain biometric identifiers or biometric information from any individual unless Sedgwick has first:

(d) Informed the individual in writing of the specific purpose and length of time for which the biometric data is being collected, stored, and used;

(e) Received a written release from the individual (or the individual's legally authorized representative) authorizing Sedgwick's collection and use of the biometric data.

Sedgwick will collect biometric data only for the specific, documented purposes disclosed to the individual at the time of collection.

Sedgwick will not sell, lease, trade, or otherwise profit from any individual's biometric identifiers or biometric information.

## RETENTION SCHEDULE

Sedgwick will retain biometric identifiers and biometric information only as long as necessary to fulfill the purpose for which the data was collected, subject to the following schedule:

(a) Pre-Employment Identity Verification Data (e.g., TruePic):

- Biometric identifiers (facial geometry scans), selfie images, government ID images, and geolocation data: Retained until the earlier of (i) the date the purpose for collection is satisfied (i.e., the hiring decision is finalized for the applicable position, plus 90 days for dispute resolution), or (ii) three (3) years from the date of the individual's last interaction with Sedgwick.
- Consent records and verification results: Retained for a minimum of four (4) years from the date of collection, to satisfy recordkeeping requirements under applicable employment and AI-related laws (including Illinois Human Rights Act amendments and California FEHA regulations).

(b) Employee Biometric Data (e.g., access control, timekeeping):

- Retained until the earlier of (i) the date the purpose for collection is satisfied (e.g., termination of employment, plus 90 days), or (ii) three (3) years from the date of the individual's last interaction with Sedgwick.

(c) Vendor-Held Data: Sedgwick requires its vendors that process biometric data on Sedgwick's behalf to adhere to retention periods no longer than those set forth in this policy. Vendor contracts include data processing agreements requiring deletion of biometric data upon Sedgwick's instruction or upon expiration of the applicable retention period, whichever occurs first.

## DESTRUCTION GUIDELINES

Upon expiration of the applicable retention period, or upon the individual's earlier request for deletion (where permitted by law), Sedgwick will permanently destroy the biometric data within thirty (30) days.

Destruction methods must render the biometric data permanently unrecoverable. Acceptable methods include:

(f) For electronic data: secure deletion using industry-standard data sanitization methods, cryptographic erasure, or physical destruction of storage media.

(g) For paper records (if any): cross-cut shredding or incineration.

Sedgwick will direct its vendors to certify in writing that biometric data has been destroyed in accordance with this policy upon request.

## SECURITY

Sedgwick will store, transmit, and protect biometric identifiers and biometric information using reasonable security measures at least equivalent to, and in the same manner as, the measures used to protect other confidential and sensitive information, including:

(h) Encryption of biometric data in transit and at rest;

(i) Access controls limiting access to biometric data to authorized personnel with a business need;

(j) Audit logging of access to biometric data;

(k) Regular security assessments of systems storing biometric data.

Vendor systems that process or store biometric data on Sedgwick's behalf must meet Sedgwick's information security standards as set forth in the applicable data processing agreement.

## DISCLOSURE RESTRICTIONS

Sedgwick will not disclose, sell, lease, trade, or otherwise disseminate any individual's biometric identifiers or biometric information to any third party unless:

(l) The individual (or the individual's legally authorized representative) provides separate written consent to the disclosure;

(m) The disclosure completes a financial transaction requested or authorized by the individual;

(n) The disclosure is required by federal, state, or local law, court order, or legal process; or

(o) The disclosure is required to protect against or prevent actual or potential fraud, criminal activity, claims, or other liability.

## INDIVIDUAL RIGHTS

Individuals may request deletion of their biometric data at any time by contacting Sedgwick at dataprotection@sedgwick.com. Sedgwick will permanently destroy the data within thirty (30) days of receiving the request, unless retention is required by law.

Individuals may request information about whether Sedgwick possesses their biometric data and the purposes for which it is used by contacting dataprotection@sedgwick.com.

Additional rights may be available under applicable state law (e.g., California CCPA rights to access, correct, and delete personal information).