Policy Name	Data Retention and Deletion Policy
Responsible Party	David Trost
Contact	privacy@compto.com
Status	Under Review
Effective Date	
Revision Date	February 2025

Compto Public Benefit Corporation Data Retention and Deletion Policy: Compliance and Supervisory Procedures

1. Introduction

By adhering to this **Data Retention and Deletion Policy**, the organization ensures compliance with U.S. anti-money-laundering regulations and consumer privacy laws, safeguards individual privacy rights, and mitigates the risks associated with excessive data storage. This policy aligns our operational practices with the principle of collecting and retaining only what is necessary, for only as long as it is needed, and then securely deleting it when obligations or business needs no longer apply.

2. Purpose and Scope

This policy establishes the standards and procedures for:

1. Retaining data in compliance with applicable legal and regulatory requirements (e.g., anti-money-laundering laws).
2. Ensuring individuals' privacy rights are respected (e.g., under consumer privacy laws such as the California Consumer Privacy Act [CCPA] or similar state laws).
3. Defining the process for securely deleting data when retention periods expire or when lawful deletion requests are validated.

Scope:

- Applies to all personal and customer data the company collects, stores, or processes, including information such as user identities, addresses, social security numbers (SSNs), email addresses, phone numbers, usage statistics, transaction records, and app logging data.
- Covers data stored in any form, including electronic databases, cloud services, backups, and physical records (if applicable).

3. Definitions

- **Personal Data:** Any information related to an identified or identifiable individual, such as name, address, SSN, email, phone number, usage stats, or transaction details.
- **Retention Period:** The duration for which data must be kept to meet legal, regulatory, or operational obligations.
- **Deletion (or Destruction):** The process of permanently rendering data unreadable and irretrievable (e.g., secure erasure for electronic files, shredding for physical records).
- **AML Data:** Data subject to anti-money-laundering regulations, which typically include customer identification details, transaction records, and supporting documentation.
- **Data Subject:** An individual whose personal data is being processed (e.g., a customer or end-user).

4. Compliance with Relevant Laws and Regulations

1. **Anti-Money-Laundering Laws**: U.S. AML regulations generally require certain financial records (including personally identifiable information like addresses, SSNs, and transaction details) to be retained for a minimum of **five (5) years** from the date of the transaction or account closure.
2. **Consumer Privacy Laws**: Various U.S. state privacy laws (e.g., CCPA) emphasize data minimization, transparency, and the right to request deletion under certain conditions. Organizations must not retain personal data for longer than it is reasonably necessary for disclosed business purposes.
3. **Other Possible State and Federal Requirements**: Laws vary by state and sector. Depending on your industry or location, you may also need to comply with:
    - **Gramm-Leach-Bliley Act (GLBA)** if handling financial data.
    - **State-Specific Data Protection Laws** (e.g., Virginia, Colorado, Connecticut), which mirror or expand upon CCPA.

Note: The exact retention timeline for non-AML data may vary based on the business's operational needs and the sensitivity of the data. However, any retention must align with a lawful purpose, and data should be deleted or anonymized once no longer needed.

5. Data Classification

To properly enforce retention and deletion, data is classified into categories:

1. **AML-Critical Data**: Personal information (like name, address, SSN) and transaction logs subject to mandatory 5-year retention under AML/BSA (Bank Secrecy Act) regulations.

2. **User Account Data (Non-AML)**: Contact details (email, phone) and basic profile information stored in the user's account.
3. **Transactional and Usage Data**: App usage statistics, purchase history, and other logs used to improve services or troubleshoot issues but not tied to AML compliance requirements.
4. **Marketing Data**: Communication preferences, email addresses for newsletters, and similar data (retention guided by user consent and the principle of data minimization).

6. Retention Schedules

The following general retention periods apply, unless superseded by stricter legal requirements:

AML-Critical Data:

Minimum **5 years** from the date of the final transaction or the closure of the account (whichever is later). This includes any information needed to verify the customer's identity and all transaction records that could be relevant for AML reviews.

User Account Data (Non-AML):

Retained for as long as the individual maintains an active account, plus a **1-year grace period** post-account closure to handle disputes or regulatory inquiries. If no regulatory or contractual obligations remain, the data is deleted or anonymized after that period.

Transactional and Usage Data (Non-AML)

Retained for operational and analytical use (e.g., product improvement) for up to **2 years**, unless there is a continued legitimate business or legal requirement. Aggregated or anonymized data may be retained indefinitely, provided it cannot be linked back to an individual.

Marketing Data:

Retained until the individual opts out or withdraws consent, or until it is no longer relevant for marketing purposes (usually **2 years** from last interaction).

7. Data Deletion Process

Scheduled Deletions:

Systems and databases must have automated or manual procedures to identify records that have reached their end-of-retention date. When a record is flagged, it is securely erased from active systems, and, if applicable, also removed from backups following the backup retention schedule.

User-Initiated Deletion Requests:

Under certain privacy laws (e.g., CCPA), individuals can request that their personal data be deleted. Upon receiving a valid, verified request, the company will remove the user's personal data unless a specific legal exemption applies (e.g., AML retention requirements, or other legal or regulatory obligations).

Secure Destruction of Physical Records (if any):

Paper documents containing personal or AML-critical data must be shredded or destroyed beyond legibility once they reach the end of their retention period.

Deletion of Backups:

Backup media may store data past the primary system retention date. The organization ensures backups are governed by similar retention timelines, meaning data is overwritten or securely destroyed upon final expiration.

8. Exceptions and Holds

Legal Holds:

If ongoing litigation or a regulatory investigation requires certain data to be preserved beyond the standard retention period, that data must not be destroyed until the hold is lifted by legal counsel or relevant authorities.

Extension of Retention for Specific Use Cases:

In rare circumstances, the CSO or Legal Counsel may authorize data to be retained longer than standard policy if a pressing business or compliance requirement exists. Such extensions must be documented, with a rationale and an updated deletion date.

9. Enforcement and Responsibilities

Policy Ownership:

The CSO (or the designated data protection officer) is responsible for ensuring compliance with this policy, conducting periodic reviews, and updating retention schedules based on new regulations or business needs.

Department/Team Accountability (if applicable):

Each department or system owner must ensure systems are configured to meet the designated retention and deletion requirements.

Training and Awareness:

All employees handling user data must be trained on proper data retention, deletion protocols, and how to handle user requests for removal.

10. Auditing and Monitoring

Periodic Audits:

The organization conducts regular internal audits (at least annually) to confirm compliance with retention periods, verify that deletion processes are followed, and validate that no unauthorized data sets exist.

Documentation:

All records of data purges, user deletion requests, and legal hold directives are logged and maintained to demonstrate compliance.

11. Review and Revisions

Review Cycle:

This policy is reviewed at least once per year or whenever there are substantial changes in applicable laws (e.g., new state privacy regulations).

Version Control:

Each revision is documented, with details on the nature of changes and the date they come into effect.

List of Revisions

Revision	Revision Date	Effective Date	Description of Changes	Approved By
v1.0	January 2025	January 2025	- Initial Release	David Trost
v1.1	February 2025		- Switch to md - add revisions - fix approval	

12. Senior Manager Approval

I have approved this Data Retention Policy as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of data retention standards and regulations.

Signed:
Name:

Title:
Date: