Data Retention Policy

Policy Owner : Bobby Das (Functional Head - Technology)

Published – 1st May 2025

Version 3

1. Introduction

2COMS Consulting Private Limited (hereafter referred to as “2COMS”) fully ensures the privacy and security of all personal data it handles. This Data Retention Policy defines how 2COMS actively manages and retains personal data collected as part of its services. It confirms the specific retention periods for personal information and the precise procedures consistently followed when data is no longer required.

2. Data Retention Principles

Data Retention Understanding:

Any data received, processed or retained by 2COMS will be evaluated subject to the business service from which it originated on case-to-case basis. Any information critical to legal, financial, regulatory compliance, related to government services or agencies or part of operational continuity will be considered as active data. This data will continue to be retained till it has been verified and approved by its data owner and/or the stakeholders. This duration might extend beyond the standard retention period of seven calendar years and will not be deleted or de-identified. Some data retention where 2COMS is the data owner, might continue till perpetuality wherever applicable. This will include data originated from or related to but not limited to

- any billable service provided where resource identity is uniquely used to qualify the billability of the service.
- any data processed where a billable service is exchanged and resource information is required by 2COMS to be retained for compliance or as proof of service provided.
- any onboarding or employee related information processed where 2COMS or its subsidiaries are the employers or involved in the employment process performing any part from pre-onboarding to post exit formalities.
- any data related to or required for fulfilment of regulatory compliance services
- any data related to any legal formalities or involved with law enforcement; government associated requirements and services or any other similar agency.
- any data sourced by 2COMS, which is not shared by customer, explicitly customer owned as per any agreement and/or not under any legal binding to be under co-ownership with any other party.

Any data outside this above or other applicable segments, will be considered for data anonymization and subsequently purging after a span of seven calendar years post operational period ends unless affirmed by 2COMS under a legally binding agreement specifying a lesser or longer period of retention.

Retention Period:
2COMS retains personal information strictly for as long as it is necessary to fulfill the purposes defined in our Privacy Policy. Once data ceases to serve these purposes, it is deleted or anonymized from active databases. In circumstances requiring longer retention, 2COMS continues to securely store personal data in compliance with legal, operational, financial, or regulatory obligations.

Retention Period for Legal Compliance:
2COMS consistently retains personal data for durations prescribed by applicable laws, including maintaining suppression lists, preventing abuse, addressing legal claims, enforcing agreements, or

meeting tax and accounting obligations. Where required, retention extends up to seven calendar years or longer, based on legal, regulatory, or compliance directives.

3. Retention in Active and Backup Databases

Active Databases:
Personal data remains in 2COMS active databases as long as individuals continue to use our services. Once services are terminated, data is systematically deleted during the scheduled six-monthly clean-up cycle.

Backup Databases:
Deleted data from active databases is securely isolated in backup storage for three months before complete and permanent deletion. During this period, the data is fully restricted from any processing, ensuring it remains protected until removal.

4. Special Retention Periods

For tax purposes, government audits, or compliance verification, personal data is retained for the periods mandated by regulatory authorities. Once these periods expire, 2COMS ensures secure deletion in full alignment with this policy unless required to be considered active data due to any other continued obligation.

5. Data Deletion

2COMS deletes personal data immediately once no legitimate processing purpose exists, guaranteeing complete and irreversible removal from active systems.

6. Data Access and Protection

Restricted Access:
Personal data is strictly accessible only to authorized personnel whose roles require such access. 2COMS enforces strong access controls, with permissions subject to periodic reviews.

Data Protection Measures:
2COMS safeguards retained data using robust technical, organizational, and procedural protections. These include end-to-end encryption, regular backups, secure storage protocols, and continuous monitoring.

7. Data Retention, De-identification of PII and Data Purge

Retention of PII:
2COMS retains Personally Identifiable Information (PII) exclusively for purposes stated in the Privacy Policy—such as recruitment services, customer support, legal compliance, and other legitimate functions. Once the operational period ends and if the data is not involved in any other critical function, the PII is scheduled for removal from active access in strict accordance with defined timelines.

De-identification of PII:
Prior to deletion, 2COMS applies de-identification or pseudonymization techniques to ensure original PII is irrecoverable and cannot be traced back to any individual. Techniques include:

- Data Masking: Replacement of names, addresses, and contact details with random or generic values.
- Aggregation: Converting identifiable attributes into grouped data sets (e.g., age ranges).
- Data Removal: Eliminating fields unnecessary for analysis.
- Tokenization: Substituting identifiers with pseudonyms/tokens linked only via secure external systems.
- Hashing: Applying irreversible cryptographic functions (e.g., SHA-256).
- Encryption: Using AES-256 and equivalent industry standards to secure fields.

De-identified datasets may be retained for analytics, research, and statistical reporting, provided they remain fully non-identifiable.

Data Purge Process:

2COMS enforces a rigorous, multi-step purge process:
1. Identification of Data for Purging – The data management team identifies non-required data after validating retention periods, legal needs, business use and other applicable cases as listed above.
2. Stakeholder Approval – Mandatory approval is obtained from Legal, Operational, Compliance, and Financial stakeholders and Management before purging.
3. Execution – The IT team securely wipes or de-identifies data, ensuring deletion from active and backup databases.
4. Verification – Permanent deletion or anonymization is verified against internal and regulatory requirements.

If de-identified data is retained for research or analysis, it remains entirely non-traceable and is securely deleted when no longer required.

8. Accountability and Oversight

2COMS continuously reviews and audits its data retention practices to ensure compliance with all applicable laws and this Policy. Retention periods, deletion processes, and documentation are actively monitored and updated. Any revisions are communicated transparently to stakeholders and impacted individuals.

9. Contact and Data Subject Rights

Individuals may contact 2COMS at privacy@2coms.com regarding their personal data. 2COMS ensures all rights to access, correction, and deletion are upheld in full compliance with our Privacy Policy.

10. Conclusion

2COMS enforces this Data Retention Policy as an active, organization-wide standard. The company ensures that all personal data is retained only for legitimate purposes and securely deleted or anonymized thereafter, guaranteeing privacy, compliance, and trust at all stages of data handling.