POLICY DOCUMENT: DATA PRIVACY & SECURITY

Organization: NA Telecommunications & Internet Services
Department: Compliance & Information Security
Document ID: SEC-POL-2025-02
Version: 1.0
Effective Date: 10/2/2026

1.0 Purpose & Scope

This policy defines the standards for protecting customer Personally Identifiable Information (PII), proprietary account data, and payment information. It applies to all call center agents, management, and third-party processors. Adherence to this policy is mandatory to maintain customer trust and legal compliance.

2.0 Regulatory Compliance Framework

This organization operates in strict accordance with international and local data protection laws. All data handling procedures must align with:

1. **GDPR (General Data Protection Regulation):** For handling data of EU citizens.
2. **CCPA (California Consumer Privacy Act):** For handling data of California residents (where applicable).
3. **Local Telecommunications & Data Laws:** Specifically including **Egypt's Personal Data Protection Law (PDPL - Law No. 151 of 2020)** and other regional telecommunications authority mandates.
4. **PCI-DSS:** Payment Card Industry Data Security Standard for handling financial information.

3.0 Call Opening & Privacy Protocols

Transparency regarding data collection is a legal requirement.

3.1 Mandatory Call Recording Notification

Agents must clearly state that the interaction is being recorded immediately upon call connection.

- **Required Script:** *"This call may be recorded for quality assurance and training purposes."*
- **Compliance Status:** Failure to read this script verbatim at the start of the call is a **CRITICAL** violation.

3.2 Privacy Disclaimer

Agents must inform customers how their data is used when requesting sensitive information (e.g., updating a profile or processing a new contract).

- **Required Script:** *"To assist you, I need to access your account details. Please be aware that your data is used solely for service provisioning and support quality, in accordance with our Privacy Policy."*

4.0 Customer Data Handling Standards

Strict protocols govern how data is verbally communicated and documented.

4.1 Payment Information (PCI-DSS)

- **Reading Data:** Agents are **strictly prohibited** from reading full credit card numbers or bank account numbers back to the customer.
- **Verification:** Agents may only verify the **last 4 digits** of a payment method (e.g., "Ending in 4298").
- **CVV/CVC Codes:** Agents must never ask for, record, or repeat the 3-digit security code on the back of a card.

4.2 Data Redaction in Notes

- When entering Case Notes or CRM updates, sensitive data must be masked.
- **Correct:** "Customer verified via card ending in 1234."
- **Incorrect:** "Customer verified via card 4400 1234 5678 9010."

5.0 Access Controls & System Security

5.1 Role-Based Access Control (RBAC)

Access to call recordings, transcripts, and customer history is restricted based on role:

- **Agents:** Access restricted to their *own* call history and active customer cases only. No download permissions.
- **Team Leads/Managers:** Full read access to team calls and transcripts for coaching purposes.

- **QA/Compliance:** Full system access including analytics and audit logs.

5.2 Authentication Protocols

- **Two-Factor Authentication (2FA):** All system users must enable 2FA (SMS or Authenticator App) to access the CRM and Telephony systems.
- **Session Timeout:** Systems will automatically log out users after **30 minutes** of inactivity. Re-authentication is required to resume work.

5.3 Password Policy

- **Complexity:** Minimum 12 characters, including uppercase, lowercase, numbers, and symbols.
- **Rotation:** Passwords must be changed every **90 days**.
- **Prohibition:** Passwords may not be reused for 12 cycles.

6.0 Data Retention & Deletion Rights

6.1 Retention Schedule

To balance quality assurance needs with privacy minimization, data is retained according to this schedule:

Data Type	Retention Period	Action After Period
Audio Call Recordings	90 Days	Permanently Deleted
Call Transcripts	1 Year	Anonymized & Archived
Analytics/Metadata	2 years	Aggregated & Anonymized

6.2 Right to Deletion (Right to be Forgotten)

If a customer requests their data be deleted:

1. Agent must flag the account as "Data Deletion Request."
2. The request is routed to the Data Compliance Officer.
3. Verification of identity is performed.
4. All non-essential PII (recordings, transcripts) are purged within **30 days**.
5. *Note:* Basic billing records required by tax law are retained but locked.

7.0 Third-Party Data Processing (AI & ML)

We utilize **VocalMind**, an AI-driven quality assurance tool, to process call data.

7.1 Processing Architecture

- **Groq LLM:** Used for high-speed transcription and sentiment analysis.
- **Pinecone:** Used as a vector database to store anonymized conversation embeddings for trend analysis.
- **Ollama:** Used for generating local embeddings to ensure data minimization.

7.2 Data Usage Policy

- Data sent to these processors is strictly for **Quality Assurance and Training**.
- Data is encrypted in transit (TLS 1.2+) and at rest.
- No customer data is sold to third parties or used to train public AI models.

8.0 Incident Management

8.1 Breach Notification Protocol

In the event of a suspected data breach (e.g., unauthorized access, phishing success, accidental exposure):

1. **Immediate Action:** The detecting employee must notify the IT Security Desk immediately.
2. **Containment:** IT freezes relevant accounts within 15 minutes.
3. **Investigation:** Security Team determines the scope of the leak.
4. **Notification:** If PII is compromised, affected customers and regulatory bodies (e.g., Data Protection Centre) will be notified within **72 hours**.

9.0 Agent Workplace Standards

9.1 Clean Desk Policy

- No personal mobile phones, cameras, or recording devices are allowed on the operations floor.
- No paper, pens, or physical note-taking devices are permitted at the desk (all notes must be digital).

9.2 Screen & Information Sharing

- **Screen Sharing:** Strictly prohibited unless authorized by IT for technical support.
- **Credential Sharing:** Sharing login credentials with colleagues is strictly prohibited.

10.0 Compliance & Enforcement

Violations of this policy are categorized by severity and carry specific disciplinary actions.

Severity Level	Definition	Consequence
CRITICAL	Actions that cause immediate legal risk or data loss. *(Examples: Failure to read Recording Script; Intentional data leak; Reading full credit card number).*	**Immediate Suspension** pending investigation; potential termination.
HIGH	Actions that degrade security posture. *(Examples: Sharing passwords; disabling 2FA; leaving unlocked PC unattended).*	**Formal Written Warning**; removal of remote work privileges (if applicable).
MEDIUM	Procedural errors with low immediate risk. *(Examples: Incomplete redaction in notes; violation of clean desk policy).*	**Coaching Session** and re-training module assignment.

Approved by: Chief Information Security Officer (CISO)
Date: 7/2/2026