

# Regulations & Compliance Framework for Najm Contact-Centre Operations

NJM-CMP-REG-007 · Version 2.4 · Effective 01 Jul 2026

|                |                                       |
|----------------|---------------------------------------|
| Classification | Internal — Restricted                 |
| Owner          | Najm Customer Care & Compliance       |
| Prepared for   | Contact Centre, QA & Compliance teams |
| Status         | Approved · in force                   |

---

## Contents

### Purpose

1. Regulatory landscape
2. Consumer protection principles
3. Motor accident regulations
4. Personal Data Protection Law (PDPL)
5. Call recording and monitoring
6. Records retention
7. Anti-fraud obligations
8. AI governance for Conversation Intelligence
9. Service level obligations
10. Conduct and ethics
11. Compliance monitoring and breaches
12. Control mapping summary

## Revision history

| Ver.    | Date     | Change                                 | Approved by           |
|---------|----------|----------------------------------------|-----------------------|
| 1.0     | Mar 2024 | Initial release                        | Head of Customer Care |
| 2.0     | Feb 2025 | PDPL alignment, AI-assisted QA         | Compliance Officer    |
| 3.0     | Mar 2026 | Saudi dialect guidance, delay handling | Head of Customer Care |
| Current | Sep 2026 | ETA transparency and escalation rules  | Compliance Committee  |

---

## Purpose

This document summarises the regulatory, legal and internal compliance obligations that govern Najm contact-centre interactions. It is an operational reference for representatives, QA reviewers and the Conversation Intelligence platform. It is not legal advice; where a conflict exists, the official regulation text prevails.

Each obligation is mapped to a control and to the SOP step or checklist item that evidences it, so that every call can be audited end-to-end.

## 1. Regulatory landscape

Saudi Central Bank (SAMA): supervises insurance and insurance-related service providers, including consumer protection principles, complaint handling and outsourcing.

Insurance Authority (IA): oversees motor insurance market conduct and the unified compulsory motor insurance policy.

General Department of Traffic (Muroor): traffic law, accident regulations and coordination with Najm on accident scene management.

Saudi Data & AI Authority (SDAIA) / National Data Management Office: Personal Data Protection Law (PDPL) and its implementing regulations.

Communications, Space & Technology Commission (CST): call recording and telecommunications consumer rights.

Najm internal policies: Code of Conduct, Information Security Policy, Records Retention Policy, AI Governance Policy.

## 2. Consumer protection principles

Fair treatment: customers must be treated fairly, honestly and professionally at every stage of the relationship. Control: neutral, respectful language; no fault assignment by representatives (Checklist D12, I3).

Disclosure and transparency: customers must receive clear, accurate information, including timeframes. Control: ETA stated as a range; transparent explanation if unavailable (Checklist E5, E6, F5).

Protection against fraud and misuse: identity must be verified before disclosing report information (Checklist C3).

Complaints handling: every complaint must be logged, acknowledged, given a reference and SLA, and customers informed of their right to escalate to SAMA (Checklist G3-G5).

---

Vulnerable customers: elderly, injured, distressed or non-Arabic-speaking customers must receive additional support, including language assistance and call-back offers.

### **3. Motor accident regulations**

Accident reporting: drivers involved in a traffic accident must report it to Najm (in Najm-covered cities) or Muroor. Representatives must not discourage reporting.

Injuries and fatalities: any injury requires Red Crescent (997) notification; fatalities and serious injuries are handled by Muroor. Najm representatives must route immediately (SOP Step 4, Checklist B1-B2).

Moving vehicles: vehicles may be moved from the travel lane in minor, injury-free accidents to reduce secondary collisions, after documentation (SOP Step 5).

Liability determination: liability percentages are determined by the authorised surveyor or Muroor officer using the approved liability tables, not by contact-centre staff. Representatives must not speculate about fault or percentages.

Self-Report: minor accidents meeting eligibility criteria can be reported via the Najm app with mutual agreement; it must be presented as optional.

### **4. Personal Data Protection Law (PDPL)**

Lawful basis: personal data is processed to perform the accident-reporting service and to comply with legal obligations.

Data minimisation: collect only what is necessary. Representatives confirm only the last 4 digits of ID/Iqama verbally (Checklist C5).

Purpose limitation: data collected for accident reporting must not be used for marketing without consent.

Data subject rights: callers may request access, correction or deletion; route such requests to the Data Protection Office within 2 working days.

Sensitive data: health information (injuries) is sensitive; record only what is necessary for safety and the report.

Cross-border transfer: call recordings and transcripts must remain in KSA-hosted infrastructure unless an approved transfer mechanism exists.

Breach notification: suspected data breaches must be reported to the Information Security team immediately; regulatory notification within 72 hours where required.

### **5. Call recording and monitoring**

---

The IVR announces that calls are recorded for quality and training. Representatives must confirm this if asked.

Recordings and transcripts are used for quality assurance, dispute resolution, training and regulatory audit only.

Access to recordings is role-based and logged.

## **6. Records retention**

Call recordings: 24 months. Transcripts and AI analyses: 24 months. Complaint tickets: 5 years after closure. Accident reports: per Najm records policy and regulatory requirements.

Legal hold overrides retention schedules for any call under dispute or investigation.

## **7. Anti-fraud obligations**

Representatives must record red flags neutrally: inconsistent descriptions, reluctance to share plates, pressure to avoid surveyor, mismatched caller identity, repeated reports from the same mobile number.

Representatives must never accuse a caller of fraud; flags are routed to the Fraud Investigation Unit through CMS.

## **8. AI governance for Conversation Intelligence**

Human accountability: AI-generated transcripts, sentiment and QA scores are decision support; coaching actions and disciplinary outcomes require human review.

Transparency: QA reports must indicate that scores are AI-assisted and show evidence quotes.

Accuracy and bias: speaker diarisation and dialect transcription quality are monitored monthly; models are evaluated across Saudi dialects (Najdi, Hijazi, Eastern, Southern) and gender to avoid bias.

Data use: recordings must not be used to train external models without approval under the AI Governance Policy and PDPL.

Explainability: each SOP and checklist determination must cite transcript evidence.

## **9. Service level obligations**

Average speed of answer  $\leq$  20s; abandonment rate  $\leq$  5%; surveyor dispatch  $\leq$  2 minutes after report creation; complaint acknowledgment  $\leq$  24h; complaint resolution  $\leq$  5 working days.

SLA breaches must be explained to the caller transparently and logged.

## 10. Conduct and ethics

No gifts, inducements or private arrangements with callers, workshops or surveyors.

Conflicts of interest (e.g. the caller is a relative) must be declared and the call transferred.

Respectful, non-discriminatory service regardless of nationality, gender, age or religion.

## 11. Compliance monitoring and breaches

Monitoring: 100% of calls are analysed by Conversation Intelligence; 5% are reviewed by human QA.

Breach categories: Critical (safety, data protection, fault assignment), Major (missing dispatch/ETA transparency, complaint not logged), Minor (greeting, closing, soft skills).

Consequences: Critical breaches are escalated to the Compliance Officer within 24 hours. Repeated Major breaches trigger a formal performance plan.

## 12. Control mapping summary

Safety → SOP 4-5 → Checklist B1-B5. Identity & PDPL → SOP 6 → C1-C6. Transparency → SOP 13-15 → E5, E6, F3-F5. Fault neutrality → SOP 10, Section 12 → D12. Complaints → SOP 16-17 → G1-G5. Recording & retention → Sections 5-6 → K1-K2. AI governance → Section 8 → all AI-assisted QA reports.

## Appendix A — Regulatory control matrix

| ID   | Obligation                                    | Source                    | Control / evidence     | Severity |
|------|-----------------------------------------------|---------------------------|------------------------|----------|
| R-01 | Prioritise life safety on every accident call | Traffic law; Najm policy  | SOP 4; Checklist B1-B2 | Critical |
| R-02 | Escalate fire, fuel, trapped persons          | Civil Defence guidance    | SOP 4 exception; B5    | Critical |
| R-03 | Verify identity before disclosing report data | SAMA consumer protection  | SOP 6; C3              | Critical |
| R-04 | Minimise verbal personal data                 | PDPL                      | C5                     | Critical |
| R-05 | No fault or liability speculation             | Liability regulations     | D12                    | Critical |
| R-06 | Clear timeframes and ETA ranges               | SAMA disclosure principle | E5, E6, F5             | Major    |

| ID   | Obligation                             | Source                     | Control / evidence       | Severity |
|------|----------------------------------------|----------------------------|--------------------------|----------|
| R-07 | Log and reference every complaint      | SAMA complaints rules      | G3-G4                    | Major    |
| R-08 | Inform right to escalate to SAMA       | SAMA complaints rules      | G5                       | Major    |
| R-09 | Recording disclosure                   | CST; Najm policy           | IVR + agent confirmation | Major    |
| R-10 | Retain recordings 24 months            | Najm retention policy      | Section 6                | Major    |
| R-11 | Keep data in KSA infrastructure        | PDPL transfer rules        | Hosting controls         | Critical |
| R-12 | Support vulnerable customers           | SAMA fair treatment        | Language line, call-back | Major    |
| R-13 | Record fraud red flags neutrally       | IA anti-fraud              | Section 7; CMS flag      | Major    |
| R-14 | Human review of AI QA outcomes         | SDAIA AI ethics principles | Section 8                | Major    |
| R-15 | Branded greeting and closing           | Najm brand standard        | A2, H3                   | Minor    |
| R-16 | Respectful, non-discriminatory service | Najm Code of Conduct       | I3, I6                   | Major    |
| R-17 | Hold time limits                       | Najm service standard      | J1-J3                    | Minor    |
| R-18 | Accurate CMS records                   | Najm records policy        | K1-K2                    | Major    |

## Appendix B — Breach response timeline

| Breach                       | First action                                | Owner                | Deadline                   |
|------------------------------|---------------------------------------------|----------------------|----------------------------|
| Safety step missed           | Team Leader call review                     | Team Leader          | 24 hours                   |
| Personal data over-disclosed | Log incident, notify DPO                    | Representative / DPO | Immediate                  |
| Suspected data breach        | Information Security incident               | InfoSec              | Immediate; regulator ≤ 72h |
| Fault assigned by agent      | Compliance review, customer correction      | Compliance Officer   | 48 hours                   |
| Complaint not logged         | Create ticket retroactively, contact caller | Team Leader          | 24 hours                   |
| Repeated Major breaches      | Formal performance plan                     | Line Manager         | 5 working days             |

---

## Appendix C — Glossary

| Term       | Meaning                              |
|------------|--------------------------------------|
| SAMA       | Saudi Central Bank                   |
| IA         | Insurance Authority                  |
| Muroor     | General Department of Traffic        |
| PDPL       | Personal Data Protection Law         |
| SDAIA      | Saudi Data & AI Authority            |
| DPO        | Data Protection Officer              |
| CMS        | Najm Case Management System          |
| مباشر      | Najm surveyor attending the scene    |
| بلاغ       | Accident report                      |
| تقدير ذاتي | Najm Self-Report for minor accidents |
| ETA        | Estimated time of arrival            |
| CSAT       | Customer satisfaction score          |