

INSURER DATA PROTECTION & NON-COMPETE COMMITMENT

Your insurer data is **walled off**. From other insurers. From us. From the market.

Version history: v1.0 — 25 October 2026 (initial publication). v1.1 — 25 October 2026 (audit fixes). See </legal/CHANGELOG.md>

Digitaliisla Technologies Private Limited

Digitaliisla Technologies Private Limited ("Company") recognises that the claim, policy, insured, surveyor-engagement, pricing, loss-assessment, settlement, operational, and audit data of insurance companies using the DigiSurvey platform is highly confidential, competitively sensitive, and legally privileged under the IRDAI (Protection of Policyholders' Interests) Regulations and insurer-specific confidentiality obligations.

The Company hereby confirms and commits to every insurance-company customer that:

1

No Sale, Licensing, or Commercial Exploitation

The Company shall

not sell, license, or otherwise commercially exploit any insurer data — including claim records, insured data, pricing schedules, settlement ratios, surveyor-assignment patterns, loss experience, or any derivative insight — in any form, to any third party, for any consideration.

2

Strict Insurer-Tenant Isolation (No Cross-Insurer Visibility)

Each insurer's data is stored and processed within

dedicated cloud environments, enforced through logical tenant isolation, row-level security (RLS), separate per-insurer storage prefixes, and access controls. Tenant-held encryption keys (BYOK) are planned (see Security Statement §1).

No report, screen, API response, or export ever contains data from more than the one insurer that authorised it.

3

No Competitive Use or Benchmarking Without Written Consent

The Company shall — raw, aggregated, anonymised, de-identified, or statistical — to build competitive benchmarks, industry leaderboards, “market intelligence” reports, pricing comparators, or any product that monetises visibility into one insurer’s performance against another, without the specific prior written consent of every insurer whose data would contribute to such output.

4

No AI / ML Training on Insurer Data Beyond Account-Scoped Improvements

The Company shall , foundation models, cross-tenant classifiers, or any machine-learning artifact that persists beyond the specific insurer account that provided the data. Account-scoped OCR fine-tuning — limited to improving extraction for that insurer’s own documents — is permitted only with that insurer’s explicit opt-in and is isolated to that account’s model instance.

5

Purpose-Limited Processing

Insurer data shall be processed only for the — survey allocation, claim handling, OCR extraction, report generation, billing against that insurer, support, security, regulatory compliance, and audit response. Any other purpose requires a written amendment signed by the insurer.

6

Access Minimisation

Access to insurer data by Company personnel is . No employee has blanket access to any insurer tenant. Every access is attributable, auditable, and reviewable by the insurer on request.

7

Sub-Processors on a Need-to-Know Basis

Where sub-processors (hosting, storage, OCR, email, security, backup) are engaged, access is limited to what is strictly necessary and governed by equivalent confidentiality terms. The current sub-processor list is

published at /legal/subprocessors, with _____ for any addition and the insurer's right to object under the DPA.

8

India Data Residency for Primary Processing

All primary insurer data is stored and processed within _____. Nothing crosses borders without disclosure in our Sub-Processors list and the specific contractual safeguards (Standard Contractual Clauses or equivalent) required by DPDPA 2023 and IRDAI data-governance guidance.

9

Breach Notification — Insurer First, 24 Hours

If a personal-data breach affecting an insurer's data is detected, the affected insurer will be notified _____, with the full regulator notification cycle (CERT-In 6 hours, Data Protection Board 72 hours) following thereafter per our Breach Notification SOP.

10

Audit Rights — Annual, No-Cost, on 30 Days' Notice

Each insurer customer has the right to _____ once per contract year at no additional cost, on 30 days' written notice, including documentary audit of access logs, sub-processor arrangements, security controls, and incident records. Additional audits following a reportable incident are at the Company's cost. The auditor shall sign the Company's standard NDA, shall not disrupt the Company's operations, shall not access any other customer's data, and shall limit scope to the Services provided to the requesting insurer. Mirrors DPA Clause 12.4.

11

Return or Deletion on Termination

On termination of services, insurer data is either _____ within 90 days, at the insurer's election, subject only to the IRDAI-mandated 7-year retention for records required for insurer audit tail (held under legal hold, inaccessible for operational use).

12

Regulatory Carve-Out

Nothing in this commitment shall prevent the Company from disclosing information where required by applicable law, court order, or regulatory

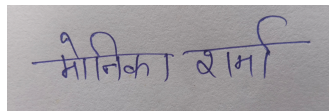
authority (including IRDAI, DPBI, CERT-In, or lawful enforcement). The Company will
and limit disclosure to the minimum lawfully required.

COMPANY COMMITMENT

Digitaliisla Technologies Private Limited's **fundamental position** is that insurer data is **not a product, not a market signal, and not an asset of the Company**. Each insurer's information remains, at all times, that insurer's property; the Company holds it in trust, uses it only for the purposes that insurer has specifically engaged us for, and keeps it operationally and visibly walled off from every other insurer and from any commercial use whatsoever.

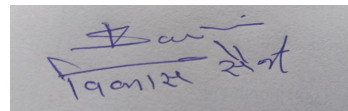
This commitment may be provided to the legal, procurement, information-security, and audit teams of any insurance company as evidence of the Company's insurer-data-protection principles. It is reinforced by Clauses 2.3, 7, and 9 of our Data Processing Agreement, the Security Statement, and the Zero-Commercial-Use Pledge, and may be enforced before the courts at Jaipur / Jhunjhunu, Rajasthan, India. Any wilful breach of this commitment carries **uncapped liability** under the DPA.

FOR AND ON BEHALF OF DIGITALIISLA TECHNOLOGIES PRIVATE LIMITED



Mrs. Monika Sharma

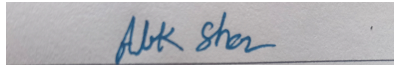
Director · Authorised Signatory
(per Board Resolution to be executed at the first
Board Meeting of the Company (ref
DIISLA/BR/2026-10-25/01 and /02 pending
signatures))



Mr. Vikas Saini

Director & Founder

WITNESSED BY GRIEVANCE OFFICER



Mr. Alok Sharma, Advocate

Grievance Officer · Bar Council of Rajasthan, Enrolment No. R/1387/2012
grievance@digitaliisla.co.in · +91 93145 91361

Dated: 25 October 2026 · Jhunjhunu, Rajasthan, India

CIN U62011RJ2026PTC119030 · Registered office: Khemi Sati Road, Jhunjhunu, Rajasthan –
333001 · legal@digitaliisla.co.in · +91 83026 98307