Muruj Alahillah Company (Loura)
Al Muhandis Mussaed Al Anqari St., Al Sulaimaniyah Dist.
Building 7965, Riyadh 12445, Kingdom of Saudi Arabia
CR No. 7052947392 · Capital: SAR 10,000

شركة مروج الأهلة
شارع المهندس مساعد العنقري، حي السليمانية
مبنى 7965، الرياض 12445، المملكة العربية السعودية
س.ت. 7052947392 · رأس المال: 10,000 ر.س

CS-POL-02 • Public

Customer Privacy Notice

Version and status

Version	Status	Effective	Owner
1.0	Finalized	01/09/2026	Chief Technology Officer

Disclaimer

This notice is issued by Muruj Alahillah Company (Commercial Registration No. 7052947392), which operates under the Loura name. It is maintained by the Chief Technology Officer and takes effect on the date shown above once approved.

Only the version published at https://loura.com/privacy is current. Printed copies, exported copies and copies held in a customer's own records are uncontrolled and may be out of date.

This notice is classified Public

1. What this notice covers

Loura makes software that automates case handling. When something needs investigation — a support escalation, a billing dispute, a compliance incident, an operational exception — Loura reads the relevant records in a customer's own systems, investigates the case using that customer's data and procedures, and proposes the response. Doing that means we handle information, and some of it is about people.

This notice explains what information we process, how it reaches us, why we use it, where it is held, how long we keep it, how AI features use it, what happens if something goes wrong, and what you can ask us to do.

It is written for two audiences. If you are a customer, or considering becoming one, it tells you how we handle information you and your people give us. If you work at a company that uses Loura, it tells you how information about you may reach us — *which can happen through an integration, without you ever using our software*. **Section 6.3** is the part that applies to you.

2. Our baseline commitments

Customer control. Customers decide what content they submit and which workflows Loura is authorised to run on it.

Purpose limitation. We use information only to provide, secure, support and administer the Services, to follow documented customer instructions, and to meet legal obligations.

Data minimisation. We take the minimum information reasonably needed for each purpose. Operational and case data is the product — that is what the Services exist to process. But where a connected system holds personal data a workflow does not need, we restrict what is retrieved at the point of collection rather than asking a customer to filter their systems first. See section 6.3.

No AI training. Neither Loura nor its providers uses Customer Content to train, retrain, fine-tune or improve shared, general-purpose, provider-owned or cross-customer AI models. Quality evaluation happens per customer, on that customer's own runs, solely to provide the Services to that customer. See section 11.1.

Security by design. We apply organisational, administrative and technical safeguards across the information lifecycle, proportionate to the risk.

Transparency and rights. We explain our roles, our providers, where information is held, how long we keep it and how to reach us, and we support the rights individuals have.

3. How this notice relates to customer agreements

This notice describes our current practices. It is not an order form, a service-level agreement, a data processing agreement or a security schedule. It does not by itself create service credits, indemnities, liability caps, warranties or audit rights.

Where a signed agreement covers the same ground, **the agreement prevails**. An agreement may add stronger or more specific protections; it cannot reduce rights that cannot lawfully be limited. Changing this notice does not amend an agreement.

This notice creates no rights for third parties beyond those the law already gives them. No system can be guaranteed completely secure or continuously available.

4. Scope and terms used

This notice applies to Loura's website, hosted software-as-a-service offering, demonstrations, integrations, support channels, customer portal, sales activities and related security operations — together, the **Services**.

- **Customer.** An organisation that evaluates, buys or uses the Services.
- **Customer Content.** Prompts, inputs, files, connected records, retrieval data, embeddings, outputs and other material submitted to, generated through or derived from use of the Services for a customer.
- **Customer Personal Data.** Personal data within Customer Content that Loura processes for and on behalf of a customer.
- **Security Incident.** An actual or reasonably suspected unauthorised acquisition of, access to, use, disclosure, alteration, loss or destruction of Customer Content within systems Loura controls.
- **Controller**, **Processor**, **Data Subject**, **Personal Data**, **Sensitive Data**, **Processing** and **Personal Data Breach** carry the meanings given under the Personal Data Protection Law of Saudi Arabia and its Implementing Regulation.

This notice does not describe a customer's own privacy practices, and it does not replace a separate workforce or recruitment notice.

5. Loura's privacy roles

When we act for a customer. For Customer Personal Data processed on a customer's documented instructions, the customer decides the purposes and means, and Loura acts as

Processor. We do not decide new purposes for that data. Customer Content appearing in support material, logs, prompts or outputs stays subject to the customer's instructions unless we identify a separate purpose of our own and say so.

When we act for ourselves. Loura is Controller for business-contact, account-administration, website, commercial, billing, support-management and service-security information. In that role the notice obligation and the rights response are ours.

Which role applies. One person can appear in both. Your account and relationship details are usually controlled by Loura; what you enter into your employer's workspace is usually controlled by your employer. We route requests according to which is which, and we tell you which route your request took.

6. Information we process

6.1. Information given to us

- **Account and identity data.** Name, business contact details, organisation, role, account identifiers, authentication records, permissions.
- **Commercial and transaction data.** Contracts, order and billing contacts, invoices, payment status, related correspondence.
- **Support and communications.** Tickets, emails, meeting notes, session records where disclosed, feedback.
- **Customer Content submitted directly.** Prompts, inputs, files and other material a user provides.

6.2. Information generated by use of the Services

- **Service and technical data.** IP address, device and browser information, timestamps, feature usage, API events, tenant identifiers, diagnostics, configuration metadata.
- **Security data.** Authentication, access and administrative activity, alerts, indicators, vulnerability and incident records, audit evidence.
- **Essential website data.** Session, authentication, security and essential preference identifiers needed to run the website and Services.
- **Outputs and derived material.** Results the Services generate; derived forms such as embeddings and index entries; and run traces — a step-by-step record of each case a workflow handles, including the prompts sent to and outputs received from AI models, kept for audit, quality and security purposes. See sections 11 and 13.

6.3. Information that reaches us through a connector

This is the section that may apply to you if you have never used Loura.

Loura connects to systems a customer already runs: case intake channels (email inboxes, forms, ticketing), CRM, ERP and ITSM platforms, document stores holding procedures and case history, and other integrations documented in that customer's agreement. These are operational systems. They also routinely hold information about people:

- Customers, complainants and correspondents named in tickets, emails and case records — including anyone who writes to a monitored intake channel
- Employee and contractor records sitting in the same ERP or CRM instance as the operational data — which can include identification numbers, employment terms, absence records and payroll details
- Attribution in operational and case records: who handled the case, who approved a decision or deviation, whose electronic signature closed a record. In regulated industries this is often mandatory and cannot be removed
- Named individuals in quality, dispute, deviation and non-conformance records
- Technician and agent names, certifications and competency records
- Badge, turnstile and time-and-attendance logs, which at some sites include biometric enrolment
- Health and safety incident and injury records
- Driver, contractor and supplier-contact details in logistics and procurement records, including sole traders whose business record is the person
- Free-text fields (handover notes, comments, remarks) which can contain anything

If you work at, or correspond with, a company that uses Loura, information about you may reach us this way even though you have never used our software and have never sent us anything. Because Loura watches a customer's intake channels so that no case is missed, this includes cases that no configured workflow handles: those are counted and returned to the customer's ordinary manual process.

What we do about it. Before a connector is switched on, we assess what personal data it can reach and restrict the connection to the records and fields the workflow actually needs. Where a connector could reach categories needing additional protection — *health, biometric, criminal or children's data* — activation is held until that access is either removed or specifically approved with a lawful basis recorded.

Connections operate from inside the customer's own network, and credentials for the customer's systems stay there — they never reach Loura. Reads are limited to the records and fields the authorised workflow needs. Nothing is written back to a customer's systems by the AI directly: every change passes controls that determine whether human approval is required first, and every change is recorded with a complete audit trail. Each connection is documented — its purpose, data categories, permissions, direction, frequency, retention and security responsibilities — and retrieved data is used only for the authorised workflow.

We do not ask customers to filter their own systems before connecting them. The safeguard sits in how each connection is scoped: what the worker may read is assessed and restricted before activation, not left to whatever the underlying system would allow.

Approving a connector does not authorise access to or control of PLC, SCADA, DCS, SIS, MES or other operational-technology and production-control systems. Any future OT connectivity requires a separately signed scope, architecture, security and safety assessment first.

7. How information is collected

Information reaches us directly from customers and authorised users; automatically through use of the Services; from customer-approved administrators, ERP systems, internal platforms and connectors; from providers acting for us; and from lawful public or professional sources.

Where Loura is Controller and obtains personal data indirectly rather than from you, we provide the required notice without undue delay and no later than 30 days, subject to lawful exceptions.

8. Why we process information, and on what basis

- **Provide and administer the Services.** Create tenants, authenticate users, run configured workflows, deliver outputs, provide support.
- **Protect customers and the Services.** Prevent misuse, investigate suspicious activity, keep security records, enforce access controls, respond to incidents.
- **Operate and improve reliability.** Diagnose faults, plan capacity, improve usability, using minimised or irreversibly anonymised information where we can.
- **Manage the relationship.** Contracts, billing, service changes, training, operational communications.
- **Comply and defend.** Legal, accounting and audit obligations, lawful requests, establishing or defending claims.

The legal basis depends on the activity. It may be consent, performance of an agreement, compliance with a legal obligation, protection of an individual’s actual interest, a documented legitimate interest that does not override individual rights, or another basis the law permits.

9. Controller processing summary

Where Loura acts as Controller:

Activity	Personal data	Purpose	Required?	Recipients and locations	Retention
Account administration	Contact, role, account and authentication data	Administer access and the relationship	Required for account access	Google Cloud and authorised business providers; Saudi Arabia and lawful provider locations	Account or relationship duration, plus legal and security needs
Website operation	Device, browser, session and essential preference data	Operate, authenticate and protect the website	Required for secure operation	Google Cloud and security providers	Session duration or security need
Support management	Contact, ticket, diagnostic and communication data	Resolve requests and record service support	Required to investigate the request	Authorised support, communications and hosting providers	Until the request and related service need end, subject to legal needs
Service security	Authentication, access, audit, alert and incident data	Protect the Services and investigate misuse	Required for secure use	Google Cloud, security advisers, and competent authorities where required	As long as reasonably needed for monitoring, investigation and legal accountability
Commercial and billing	Contract, billing contact, invoice and payment-status data	Contract administration, accounting, legal compliance	Required for contracting and payment	Authorised accounting, banking and professional advisers	Applicable statutory, tax and claims periods

10. Customer Content, ownership and confidentiality

As between Loura and a customer, the customer keeps its rights in its content — *records, recipes, processes, workflows, business rules and confidential information*. Loura receives only the limited rights needed to provide, secure and support the Services, follow instructions and meet legal obligations.

We do not sell or rent Customer Content. We do not use one customer's confidential information to build something for another. Access is limited to authorised personnel and approved providers who need it and are under confidentiality obligations.

Ownership of the product, customer-specific deliverables, feedback and pre-existing intellectual property is governed by the signed agreement.

11. AI and automated processing

11.1. How AI features use information

AI features process Customer Content only to deliver functionality the customer has selected or instructed.

Neither Loura nor any provider uses Customer Content to train, retrain, fine-tune or improve shared, general-purpose, provider-owned or cross-customer AI models. We engage AI model providers only under terms that prohibit training on Customer Content. Loura evaluates the quality of a customer's own runs, within that customer's tenant, solely to provide, secure and support the Services for that customer; those evaluations are never used to build or improve models or services for anyone else.

Loura and provider personnel access prompts, inputs or outputs only where authorised for support, security, abuse investigation or legal compliance, under access and confidentiality controls.

AI output can be incomplete, inaccurate or inappropriate. Apply human review and independent validation before acting on it in any consequential way.

11.2. Automated decisions and effects on individuals

Depending on the capabilities configured by the customer, the Services may generate outputs that relate to or affect an identifiable individual. For example, an output may assign work to a person, attribute an event or action, identify an error or exception, flag a record for review, recommend a response, or initiate or escalate an action concerning an individual. Such processing is performed according to the customer's configuration, procedures, permissions and controls.

12. Providers, hosting and locations

Loura hosts the production Service on Google Cloud in the Dammam region, Saudi Arabia (me-central2). Google Cloud acts as a Subprocessor for applicable Customer Personal Data. The

contracting entity, services, processing locations, support access and Google's own subprocessors are governed by Loura's Google Cloud contracting documents and provider register.

AI model inference is provided through one or more AI model providers recorded in our provider register, acting as Subprocessors. We engage them only under terms that prohibit use of Customer Content to train their models, and we select zero-retention or no-storage configurations where the provider offers them; where a provider retains prompts and outputs for abuse or safety monitoring, that retention is limited — currently no more than 30 days — after which the content is deleted. Depending on the models a customer selects, inference may be processed outside Saudi Arabia; the locations for each configuration are recorded in our data-flow records, and the transfer safeguards in this section apply. Customers with stricter requirements can run an approved model inside their own network, in which case prompts and outputs do not leave it.

Where a customer chooses to receive notifications through its own communication channels. the case information in those notifications is delivered to the channel provider the customer selected, on that customer's instruction.

We use providers only for documented service, infrastructure, identity, communications, security, billing or professional purposes. They receive the minimum information necessary and are bound by privacy, security, incident, confidentiality and deletion obligations.

Before appointing or replacing a subprocessor for Customer Personal Data, we give the notice, acceptance and objection opportunity that the law and the signed agreement require.

Locations. Primary production hosting is configured in Dammam. Regional hosting does not by itself mean every support, telemetry, administrative-access or onward-processing activity stays inside Saudi Arabia; we record those activities in our provider and data-flow records.

Where Loura is Controller, we assess purpose, necessity, destination, recipient, mechanism and risk before transferring personal data outside Saudi Arabia. Where Loura is Processor, we transfer only on documented customer instructions and with the required safeguards. We stop a transfer if the required protection cannot be maintained.

Subprocessor and connector approval gates are held in [CS-POL-03] Third-Party and Cloud Computing Policy [to be issued].

13. Retention and deletion

We keep information only while it is reasonably needed for the documented purpose, the signed agreement, security, legal obligations and claims. Retention runs by category and trigger, not one blanket period.

Customer Content is kept while needed to provide the Services and through the export or deletion window in the agreement.

Deletion. At the end of the applicable period, information is securely deleted, made inaccessible, or irreversibly anonymised.

Derived information. When information is used as context for an AI feature, a derived form may exist — an embedding or index entry. It is not a copy in the ordinary sense, but it can still relate to a person, so we treat it as personal data. Derived forms are stored alongside their source in the same tenant-isolated store, so when source information is deleted, derived forms built from it are deleted or rebuilt without it in the same deletion cycle

Backups. Deleted information is put beyond ordinary use and removed through the protected backup-expiry cycle, which completes within 35 days at most. If a backup is restored, deletion requests and expiry rules are reapplied.

Legal holds. Deletion can be suspended for a specific legal, regulatory, audit or dispute obligation. Access stays restricted, and deletion resumes when the obligation ends.

Pseudonymised or de-identified information is still personal data where re-identification is reasonably possible. It is treated as non-personal only after irreversible anonymisation.

14. Security

Loura runs a risk-based cybersecurity programme covering governance and people, identity and access, data and platform security, secure development, resilience and supplier management. Controls are chosen according to the sensitivity of the information, the architecture of the Services, threat exposure, contractual commitments and applicable law.

Specific control commitments, their scope and the evidence behind them sit in the security schedule to a customer's agreement rather than in this notice, because they are contractual and change over time. Security questionnaires, assessment summaries and test summaries can be provided under appropriate confidentiality protections. No system can be guaranteed completely secure.

15. If something goes wrong

For an actual or reasonably suspected Security Incident materially affecting Customer Content or the Services, we give the affected customer preliminary notice **without undue delay**. We do not hold back an initial notice because the investigation is incomplete, and we provide updates as facts emerge.

Where Loura is Controller, we assess whether a Personal Data Breach meets the threshold for notifying the competent authority or affected individuals. Qualifying notifications are made within 72 hours of becoming aware, and individuals are notified without undue delay where the statutory threshold is met.

Where Loura is Processor, we support the customer's assessment, notices and response, preserve evidence, and do not notify a regulator or individual on the customer's behalf unless instructed or legally required.

16. Your rights and how to exercise them

You can:

- **Be informed.** Know who the Controller is, the purpose and basis, whether providing information is required or optional, how long it is kept, who receives it, and what rights you have.
- **Access and obtain a copy.** Confirm whether we hold personal data about you and receive it in a readable format, subject to lawful protections.
- **Correct, complete or update.** Ask us to fix data that is inaccurate, incomplete or out of date, and to tell recipients where required.
- **Request destruction.** Ask us to delete, subject to lawful retention exceptions.
- **Withdraw consent.** Where we rely on consent, withdraw it. This does not affect processing already carried out lawfully.
- **Complain and seek remedies.** Raise it with us, and with the competent authority or through a legal remedy.

How to ask. Email privacy@loura.com. Tell us the Service or the customer organisation involved, what you are asking for, and enough detail for us to find the record. We verify who you are using proportionate information — please do not send passwords or unnecessary identity documents.

If the information sits in your employer's workspace, your employer is usually the Controller. We route the request to them and assist under the applicable agreement, and we tell you we have done so.

Timing. We act without delay and within 30 days. If we need an extension, it will be no more than one further 30-day period, and we will tell you in advance and explain why.

If you are not satisfied. You can escalate to the Saudi Data & AI Authority through its Data Governance Platform. A complaint can generally be submitted within 90 days of the incident or of becoming aware of it, and a later complaint may be accepted for reasonable cause.

17. Cookies and communications

Loura uses cookies and similar technologies, including analytics and marketing tools, to understand how visitors use our website and Services, measure performance, improve functionality, and support our marketing activities. We also use technologies necessary for authentication, security, session management, user preferences, and the operation of our Services.

Loura may send direct-marketing communications where permitted by law. Recipients may unsubscribe from these communications at any time using the link provided in the message or by contacting us.

Operational, contractual, billing, support, and security communications are necessary service messages and are not considered marketing.

Where required by applicable law, we will obtain consent before using non-essential cookies or similar technologies and provide appropriate mechanisms for users to manage or withdraw their consent.

18. Sensitive data and individuals requiring additional protection

The Services are built for organisational use and are not directed to children. We do not seek children's personal data.

Sensitive data can still reach us — health and injury records, biometric enrolment in access systems, and similar categories held in the operational systems we connect to. Section 6.3 explains how that happens and what we do about it. Prohibiting customers from **submitting** these categories does nothing about a connector **ingesting** them, so the safeguard is the connector gate, not an instruction to customers.

Where higher-risk processing is approved, it gets additional notice, consent, minimisation, access, assessment and security controls appropriate to the risk and the law.

19. Changes to this notice

We review this notice periodically, and when the Services, the law, technology or our practices change materially. We record material revisions and the effective date of each version. The current approved version is published at https://loura.com/privacy. Material changes are communicated through the Services, by email, or another reasonable channel where required.

20. Contact and complaints

Purpose	Contact
Privacy questions, rights requests, complaints	privacy@loura.com
Cybersecurity questions and vulnerability reports	security@loura.com
Contractual and service requests	support@loura.com

End of document