



LAKEORA Privacy Policy

Effective Date: 1 May 2026

Last Updated: 1 May 2026

Version: 1.0

1. About LAKEORA

LAKEORA is a Saudi Arabian information technology company providing Databricks-related consulting, implementation, and assurance services to public- and private-sector customers.

Legal name: LAKEORA Company, a Simplified Joint Stock Company

Unified National Number: 7053815200

Registered address: Building 3385, Al Thumamah Street, Al Nada District, Riyadh 13317-8398, Kingdom of Saudi Arabia

Website: <https://www.lakeora.ai>

Privacy email: privacy@lakeora.ai

Telephone: +966 11 495 7513

LAKEORA acts as a personal data controller when processing information for its own business purposes. When LAKEORA processes personal data solely on a customer's documented instructions, the customer remains the controller and its privacy policy governs that processing.

This Policy is structured around the Saudi Personal Data Protection Law, its Implementing Regulations, the Personal Data Transfer Regulations, and SDAIA's Privacy Policy Guideline. GDPR principles are used as supplementary practice where appropriate, but GDPR applies only where its territorial requirements are met.

2. Personal Data We Collect

Depending on the service or engagement, LAKEORA may process:

- **Identity data:** Name, national identification or residency information, date of birth, nationality, and signature.
- **Business and contact data:** Employer, position, business email, telephone number, address, and customer account information.
- **Contract and transaction data:** Proposals, contracts, licenses, invoices, payment records, and purchasing information.
- **Technical data:** IP address, device identifiers, browser information, access logs, authentication records, and cybersecurity events.
- **Usage data:** Information about the use of LAKEORA's website, support services, software, and platforms.

- **Communication data:** Emails, support tickets, meeting records, inquiries, feedback, and service communications.
- **Customer-controlled data:** Personal data supplied by customers or processed within Databricks or associated cloud environments.
- **Employment data:** CVs, qualifications, work history, references, identification documents, and employee records.
- **Sensitive data:** Health, biometric, genetic, credit, criminal, security, religious, location, or similar sensitive information, only where necessary, legally permitted, and subject to additional controls.
- **Cookies:** Necessary, preference, analytics, and marketing cookie information, as described in Section 12.

Providing some information may be mandatory to enter into a contract, meet legal requirements, verify identity, provide services, or maintain system security. Other information is optional and will be identified at collection.

3. How We Collect Personal Data

LAKEORA may collect personal data:

- Directly from individuals through contracts, forms, correspondence, support requests, meetings, recruitment, or use of LAKEORA's services.
- From public- and private-sector customers that authorize LAKEORA to provide services.
- Through Databricks, cloud platforms, software integrations, identity providers, and support systems.
- From authorized representatives, business partners, vendors, and professional advisers.
- From public registers, websites, professional networks, and other lawful public sources.
- Automatically through cookies, server logs, monitoring technologies, and security tools.

Where information is obtained indirectly, LAKEORA will provide appropriate notice within the period required by applicable law, unless an exemption applies.

4. Purposes and Legal Bases

Purpose
Providing consulting, implementation, support, and resale services
Managing customer and supplier relationships
Account administration and authentication
Billing, accounting, and regulatory records
Technical support and incident response
Cybersecurity, fraud prevention, and system monitoring
Recruitment and employment administration
Marketing LAKEORA's services
Responding to authorities or legal proceedings
Service improvement and analytics

LAKEORA will not rely on legitimate interests to process sensitive personal data where Saudi law prohibits that basis. Explicit consent or another applicable legal basis will be obtained where required.

LAKEORA limits collection to information that is adequate, relevant, and necessary for the stated purpose.

5. Customer and Databricks Data

Customer data processed through Databricks may be governed by the applicable customer agreement, data processing agreement, and customer instructions. Databricks generally processes customer-uploaded platform data as a processor rather than under its public privacy notice.

Depending on the contractual structure:

- LAKEORA may act as controller for customer relationship and account data.
- LAKEORA may act as processor or service provider for customer-controlled data.
- Databricks or the relevant cloud provider may act as a processor or subprocessor.

Customers must ensure that their instructions and use of LAKEORA's services have an appropriate legal basis.

6. Disclosure of Personal Data

LAKEORA may disclose personal data to:

- Databricks and its authorized subprocessors.
- Cloud hosting, cybersecurity, communications, payment, support, and professional-service providers.
- Microsoft, Amazon Web Services, Google Cloud, or another underlying provider, depending on the customer-selected Databricks deployment.
- The relevant customer where LAKEORA processes data on that customer's behalf.
- Affiliates, auditors, insurers, banks, lawyers, and professional advisers.
- Saudi government, regulatory, judicial, law-enforcement, or cybersecurity authorities where legally required.
- A purchaser, investor, or successor in connection with a proposed corporate transaction, subject to appropriate confidentiality measures.

Databricks maintains a current [subprocessor list](#), which may change based on deployment and support arrangements.

LAKEORA does not sell personal data or disclose it to third parties for their independent direct-marketing purposes.

7. International Transfers and Hosting

Personal data may be stored or processed in:

- Saudi Arabia, where locally hosted systems are used.
- Europe, including the Databricks supported regions published for [AWS](#), [Microsoft Azure](#), [Google Cloud](#), and [SAP](#).
- The United States, including the Databricks supported regions published for [AWS](#), [Microsoft Azure](#), [Google Cloud](#), and [SAP](#).
- Other customer-selected locations identified in the applicable service agreement.

Before transferring personal data outside Saudi Arabia, LAKEORA will assess the purpose, necessity, destination, data categories, risks, and applicable safeguards. Safeguards may include SDAIA-approved

standard contractual clauses, binding contractual obligations, transfer risk assessments, access restrictions, encryption, and data minimization.

International transfers will be limited to the data required for the relevant purpose and implemented consistently with the Saudi Personal Data Transfer Regulations and applicable sector requirements.

8. Retention and Destruction

LAKEORA retains personal data only for the applicable business purpose and any contractual, regulatory, audit, dispute, or legal-preservation requirement. The periods below apply unless a longer period is required by law, a regulator, a sector-specific statutory or regulatory requirement applicable to the relevant industry or data category, a government customer's retention schedule, or the applicable customer agreement. SDAIA guidance expects retention periods to be identified by data category and data to be destroyed so it cannot be accessed or recovered.

Data Category
Customer contracts and account records
Financial and invoicing records
Support tickets and service communications
Technical and security logs
Marketing records
Unsuccessful applicant records
Employee records
Customer-controlled platform data

When retention ends, LAKEORA will securely delete, overwrite, anonymize, or otherwise destroy the data, including applicable copies, unless continued retention is legally required.

9. Security

LAKEORA applies administrative, technical, and organizational measures appropriate to the nature and sensitivity of the information, including where appropriate:

- Access controls and least-privilege permissions.
- Encryption in transit and at rest.

- Authentication and identity-management controls.
- Logging, monitoring, and incident detection.
- Backup, recovery, and business-continuity procedures.
- Vulnerability management and security testing.
- Employee confidentiality and security training.
- Processor and supplier due diligence.
- Data minimization, segregation, pseudonymization, or anonymization.

Third-party certifications held by Databricks, Microsoft, or another provider belong to that provider and do not constitute LAKEORA certifications. Where Microsoft services are used, processing will be governed by the applicable [Microsoft Data Protection Addendum](#), Product Terms, and configured service region.

No system can eliminate every security risk.

10. Your Rights

Subject to the Saudi PDPL and applicable exceptions, individuals may have the right to:

- Be informed about the collection and processing of their personal data.
- Access personal data held by LAKEORA.
- Obtain a readable copy of their personal data.
- Request correction, completion, or updating of inaccurate data.
- Request destruction of data that is no longer required.
- Withdraw consent without affecting processing previously undertaken or processing supported by another legal basis.
- Object to direct marketing.
- Submit a complaint to LAKEORA or SDAIA.
- Seek compensation for material or moral damage through the competent authority or court.

These rights reflect the categories identified in SDAIA's Privacy Policy Guideline.

Where GDPR independently applies, additional rights may include restriction, portability, objection, and protections relating to solely automated decisions.

11. Exercising Your Rights

Requests may be submitted to:

Department: Office of the CEO

Email: privacy@lakeora.ai

Postal address: Building 3385, Al Thumamah Street, Al Nada District, Riyadh 13317-8398, Kingdom of Saudi Arabia

Telephone: +966 11 495 7513

LAKEORA may request information necessary to verify identity and authority. LAKEORA will ordinarily respond within 30 days and may extend the period by a further 30 days where permitted due to the complexity or number of requests.

A request may be restricted or refused where required or permitted by law. LAKEORA will explain the applicable reason unless prohibited from doing so.

12. Cookies and Marketing

LAKEORA may use:

- **Strictly necessary cookies:** Required for website operation and security.
- **Preference cookies:** Remember user settings.
- **Analytics cookies:** Measure website performance and usage.
- **Marketing cookies:** Support advertising or campaign measurement.

Non-essential cookies will be activated based on the user's preferences where consent is required. Users may change their preferences through <https://www.lakeora.ai/cookie-settings>.

LAKEORA will obtain the required consent before sending direct marketing, identify the sender, provide a simple opt-out method, and stop marketing after withdrawal. Sensitive personal data will not be used for marketing.

13. Children's Data

LAKEORA's services are directed to organizations and business users rather than children. LAKEORA will not knowingly collect children's personal data for its own purposes without appropriate guardian authorization and legal basis.

Where customer-controlled data includes children's information, LAKEORA will process it under the customer's documented instructions and applicable safeguards.

14. Automated Processing and Artificial Intelligence

LAKEORA or its customers may use data analytics or artificial-intelligence technologies within Databricks environments. Where such processing involves personal data, the relevant controller must identify the purpose and legal basis and apply appropriate safeguards.

If LAKEORA makes a decision based solely on automated processing that produces a significant effect, LAKEORA will provide any notice, explanation, or human-review mechanism required by applicable law.

15. Personal Data Protection Officer

Where LAKEORA is required to appoint a Personal Data Protection Officer:

Name: Mohammad Alzaubi

Title: Chief Executive Officer

Email: privacy@lakeora.ai

Telephone: +966 11 495 7513

Address: Building 3385, Al Thumamah Street, Al Nada District, Riyadh 13317-8398, Kingdom of Saudi Arabia

Given LAKEORA's stated potential processing of sensitive data and customer datasets, the DPO requirement should be assessed before publication.

16. Complaints

Complaints or objections may be submitted to:

Department: Office of the CEO

Email: privacy@lakeora.ai

Telephone: +966 11 495 7513

LAKEORA will acknowledge and process complaints within 30 days.

If the individual is dissatisfied with LAKEORA's response, the individual may submit a complaint to the Saudi Data & AI Authority through the [National Data Governance Platform](#). Complaints to SDAIA are generally required within 90 days after awareness of the relevant incident.

17. Changes to This Policy

LAKEORA will review this Policy periodically and update it when its services, processing activities, suppliers, hosting locations, or legal obligations change. Material changes will be communicated through the website, direct notification, or another appropriate channel.

The update record will be available at <https://www.lakeora.ai/privacy>.

18. Contact

Questions about this Policy may be directed to:

LAKEORA

Building 3385, Al Thumamah Street, Al Nada District, Riyadh 13317-8398, Kingdom of Saudi Arabia

+966 11 495 7513

privacy@lakeora.ai

<https://www.lakeora.ai>