

Platform Terms of Use and Service Conditions

Document control	Details
Version	4.0
Effective Date	1 May 2026
Previous Version	3.0 - Superseded. Retained in archive only.
Entity	TraCERLab SC, a private-law company specialising in traceability technologies, digital identification, mineral intelligence, data management and mining supply-chain compliance ("TraCERLab", "we", "us", or "our")
Registered Office	TraCERLab SC, Avenue Marcel Gourdin 60, 5001 Namur, Belgium; VAT BE0758359658 www.tracerlabgroup.com
Classification	PUBLIC - CLIENT-FACING
Language	This document is executed in the English language. The English version is the controlling legal text in all respects. Where a translated version is provided, it is provided for user convenience only and does not create independent rights or obligations. In the event of conflict between a translation and this English text, the English text prevails.

LEGAL NOTICE - READ CAREFULLY BEFORE USING THE PLATFORM These Terms of Use constitute a legally binding contract between you and TraCERLab. By accessing, registering for, or using the Platform in any capacity, you confirm that you have read, understood, and agree to be bound by these Terms. **Business Use Only.** The Platform is designed exclusively for business, professional, and governmental use. By registering, you confirm that you are acting in a business, professional, or governmental capacity - not as a consumer as defined under applicable law. If you are an individual acting outside of a trade or profession, you must contact TraCERLab before using the Platform. If you have a signed Master Services Agreement (MSA) or Government Framework Agreement (GFA) with TraCERLab, those documents govern your use of the Platform to the extent of any conflict with these Terms. These Terms apply to all matters not addressed by the signed agreement.

PART I - DEFINITIONS

Article 1 - Defined Terms

Term	Definition
Platform	The TraCERLab SaaS system, including all service tiers, API services, web applications, data pipelines, AI engines, geospatial services, blockchain anchoring, and all associated portals, dashboards, and interfaces.
Services	The specific capabilities subscribed to by the User, as defined in the applicable Order Form or Service Description Annex.
User	Any individual who accesses the Platform via a registered account, whether individually, on behalf of an Organisational Account, or as a Government Authorised User.
Organisational Account	A registered entity (corporation, cooperative, mining company, NGO, partnership, or equivalent) maintaining a master account under which multiple Users operate.
Government Authorised User	An individual operating within the Platform under a Government Framework Agreement on behalf of a sovereign authority, ministry, regulatory body, or tax authority.

Term	Definition
Operational Actor	A User in a field-facing role, including artisanal miners, field inspectors, depot operators, transporters, and weighbridge operators.
Marketplace Participant	A User who engages with TraCerLab MARKET to post listings, submit RFQs, make offers, or participate in trade transactions.
Partner / Integrator	An entity authorised by TraCerLab to integrate via API keys or resell Platform access under an executed Partner Agreement.
Client Data	All data, documents, photographs, GPS coordinates, XRF readings, and other material submitted to the Platform by or on behalf of a User.
Mineral DNA Data	Geochemical XRF elemental profiles, provenance signatures, Mahalanobis distance scores, and isotopic data generated or stored in the Platform.
Traceability Record	A digital record capturing a supply-chain event and, where enabled, an associated tamper-evidence reference.
AI Output	Any score, recommendation, classification, flag, or insight generated by the Platform's AI or machine learning components, including but not limited to KYC risk scores, OCR extractions, fraud detection alerts, sanctions screening results, XRF anomaly signals, and geospatial intelligence outputs.
Mineral Passport	A structured digital identity document generated by the Platform for a specific mineral batch.
Certificate	A digitally generated document issued by the Platform recording verified attributes of a mineral batch, organisation, or supply chain event.
Blockchain Anchor	A cryptographic reference recorded through an external distributed-ledger service to support tamper-evidence checks.
Platform Evidence	Any Traceability Record, Mineral Passport, Certificate, Blockchain Anchor, or AI Output produced by the Platform.
Derived Data	Aggregated, anonymised, or de-identified insights generated through processing Client Data across multiple accounts.
Sub-Processors	Third-party providers engaged by TraCerLab to process Personal Data on its behalf. Current provider, function, location, and transfer details are maintained in the applicable Subprocessor and Transfer Register.
GDPR	Regulation (EU) 2016/679 (General Data Protection Regulation).
CCPA/CPRA	California Consumer Privacy Act, as amended by the California Privacy Rights Act (Cal. Civ. Code § 1798.100 et seq.).
MSA	Master Services Agreement - the principal enterprise commercial contract between TraCerLab and an Organisational Account.
GFA	Government Framework Agreement - the principal contract between TraCerLab and a sovereign or governmental counterparty.
DPA	Data Processing Agreement - the data protection annex incorporated into all contracts involving Personal Data.
OHADA	Organisation for the Harmonisation of Business Law in Africa.
CCJA	Common Court of Justice and Arbitration - the apex arbitral and judicial institution of OHADA, seated in Abidjan, Ivory Coast.
EU AI Act	Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence.
Beta Feature	A Platform feature identified as "Beta" in the Platform interface, provided without warranty, outside SLA coverage, and subject to the conditions in Article 13.7.
Privacy Policy	TraCerLab's Privacy Policy, published and maintained at: [https://platform.tracerlabgroup.com/legal/privacy-policy] - the authoritative document governing Personal Data collection, use, and rights.

PART II - NATURE AND PURPOSE OF THE PLATFORM

Article 2 - What the Platform Is

2.1 The Platform is a technology-based evidence generation and supply chain governance tool. It collects, records, processes, analyses, and presents data relating to mineral supply chains - including traceability, geochemical analysis, compliance verification, regulatory data exchange, and marketplace facilitation.

2.2 The Platform is an instrument for evidence generation and process automation. It is not a legal authority, certification body, regulatory agency, customs authority, financial institution, or tax collection body.

2.3 Platform Evidence is provided as data and analytical output to assist Users in making their own informed decisions. No Platform Evidence constitutes legal proof in any jurisdiction unless a competent court or regulatory authority has accepted it as such in a specific proceeding.

Article 3 - What the Platform Does Not Do and Does Not Guarantee

3.1 No Legal Authority. No Certificate, Mineral Passport, or Traceability Record constitutes:

- Official government certification of any kind;
- Legally enforceable proof of compliance in any jurisdiction;
- A customs declaration, export permit, or government document;
- A legal opinion, expert certification, or regulatory determination.

3.2 No Guarantee of Physical Accuracy. Platform records reflect data as submitted by Users. TraCerLab does not conduct physical inspections. TraCerLab cannot guarantee that data entered reflects physical reality.

3.3 No Guarantee of AI Output Accuracy. All AI Outputs are advisory outputs only. They are produced by probabilistic algorithms and may contain errors, false positives, or false negatives. They do not constitute compliance determinations and must not be relied upon as the sole basis for regulatory, legal, or financial decisions.

3.4 No Guarantee of Geochemical Match Accuracy. XRF-based Mineral DNA fingerprinting and provenance matching are based on probabilistic statistical models (including Mahalanobis distance scoring). These outputs carry inherent scientific uncertainty margins that are quantified in the Platform's published Technical Methodology Documents (Whitepaper Series: WP-03 XRF Physics and Uncertainty; WP-04 Geochemical Rosetta Engine). By relying on geochemical outputs, you confirm you have accessed and understood those uncertainty parameters. A match score is a probabilistic indicator - not a deterministic proof.

3.5 Tamper-evidence services. Where enabled, external distributed-ledger services may record a cryptographic reference associated with a Platform record. This can assist with later integrity checks but does not guarantee permanent network availability, legal validity, authenticity of the underlying data, or evidentiary status in any jurisdiction.

3.6 No Tax Collection Authority. Tax obligation calculation features (AFIO module) are calculation and reporting tools only. TraCerLab is not a tax authority, does not collect taxes on behalf of any government, and bears no responsibility for tax compliance outcomes. Calculations require human expert review and official confirmation before use in any regulatory or fiscal submission.

3.7 No financial services. TraCerLab is not a bank, payment institution, escrow agent, broker, or other regulated financial-services provider. Any payment, settlement, or escrow functionality is available only where expressly included in an applicable agreement and operated in accordance with applicable law and any required authorisation.

3.8 No Insurance. TraCerLab does not provide professional indemnity, product liability, or any other insurance product.

3.9 Data location and residency. Hosting locations, backup and recovery arrangements, and any data-residency commitment are governed by the applicable Order Form, Data Processing Agreement, Government Framework Agreement, or service-specific notice. These Terms do not promise processing or storage in a particular country or facility.

3.10 Advisory vs. Enforcement Outputs - Government Use. Where Government Authorised Users deploy Platform outputs as an input into an enforcement decision (including seizure, confiscation, tax assessment, or licence revocation), the Platform output constitutes a prima facie evidentiary indicator requiring independent human expert review and official verification. No Platform output constitutes an automated administrative decision binding on any

person under public law. Enforcement authority and legal responsibility remain exclusively with the competent government authority. TraCerLab's involvement in generating a Platform output does not constitute expert testimony, official certification, or a delegated exercise of public power - unless TraCerLab has separately and explicitly agreed in writing to provide such services under a signed professional services agreement subject to independent legal review.

PART III - REGULATORY POSITIONING

Article 4 - Regulatory Framework

4.1 TraCerLab is a Belgian-incorporated technology platform. It is subject to Belgian corporate law, GDPR, and applicable EU regulations. It is not itself a regulated entity under financial services, tax collection, customs, mining regulation, or AML law in any jurisdiction, except to the extent such laws apply to it in its capacity as a Belgian entity.

4.2 Users remain solely responsible for their own regulatory compliance, including:

- Mining sector regulations in their jurisdictions of operation
- AML/CFT obligations applicable to their own business activities
- Tax and export reporting obligations
- GDPR, CCPA/CPRA, and applicable data protection laws
- OECD Due Diligence Guidance for Responsible Mineral Supply Chains
- EU Regulation 2017/821 (Conflict Minerals Regulation)
- EU Battery Regulation 2023/1542 (as applicable)
- SEC Section 1502 conflict minerals disclosure obligations (for US-listed entities)

4.3 Explicit Regulatory Exclusions:

- Government and registry integrations. Availability of a government or registry integration does not imply approval, endorsement, delegation of authority, or a formal data-sharing relationship unless TraCerLab expressly confirms that relationship in a signed agreement.
- Country-specific modules. Platform outputs do not replace an official certificate, permit, approval, registry entry, or determination issued by a competent authority.
- EU: Platform Certificates are not CE marks, ISO certifications, or regulatory approvals of any kind.

4.4 Marketplace and regulated services. The Platform may provide technology that supports trade discovery, transaction workflows, or connections to third-party financial-service providers. TraCerLab does not provide a regulated financial service unless that service is expressly identified in a signed agreement and all required legal conditions and authorisations have been satisfied.

PART IV - ELIGIBILITY AND ACCOUNT CREATION

Article 5 - Eligibility

5.1 Business and Professional Use Only. The Platform is provided exclusively for business, professional, and governmental use. By registering, you confirm that you are acting in a business, professional, or governmental capacity. If you are an individual who is not acting in a business or professional capacity - for example, if you are a private individual with no commercial connection to the mineral supply chain - you must not register for or use the Platform without first contacting TraCerLab at legal@tracerlabgroup.com.

5.2 Consumer Rights Preservation. Nothing in these Terms restricts or excludes mandatory rights that apply to you under consumer protection law if you qualify as a consumer under applicable law despite the business-use requirement above. If you believe you may have consumer status, you may choose to resolve disputes before courts in your place of residence rather than through arbitration, notwithstanding Article 31.3.

5.3 Legal Capacity. You must be at least 18 years of age (or the age of majority in your jurisdiction), have legal capacity to contract, and not be subject to sanctions that prohibit contractual relations with Belgian entities.

5.4 KYC and KYB. Certain features - including TraCerLab MARKET, TraCerLab GOVERN, and specific TraCerLab COMPLY modules - require completed KYC and/or KYB verification. Decisions may be refused without disclosure of specific reasons where required by AML/CFT obligations.

5.5 Sanctions screening. Where screening is enabled, TraCerLab may check account and transaction information against applicable sanctions lists and other authorised sources. Screening may produce false positives or false negatives. Registration or access may be restricted while a potential match is reviewed in accordance with Article 24.

5.6 Excluded Activities. TraCerLab does not provide Services to entities or individuals subject to comprehensive sanctions programmes of the EU, US, UK, or UN.

Article 6 - Account Registration and Acceptance

6.1 Accuracy. You must provide accurate, current, and complete registration information and promptly update it. Material misrepresentation grounds immediate termination.

6.2 MFA. All accounts require multi-factor authentication enrolment. Failure to maintain active MFA may restrict access to sensitive features.

6.3 Security. You are responsible for credential confidentiality, all activity under your account, and immediate notification to TraCerLab of suspected unauthorised access.

6.4 Enterprise account management. Organisational Account administrators manage authorised users and are responsible for their compliance with these Terms. Access is restricted through role-based permissions appropriate to the relevant responsibilities and configuration.

6.5 Duress Code. The Platform provides an optional duress code mechanism for Users in high-risk field environments. Activation triggers the following specific protocol within the Platform: a timestamped alert is generated and transmitted to the Organisational Account administrator; the alert is logged in the Platform audit record. Activation does not contact law enforcement, emergency services, any government authority, or any external party of any kind. TraCerLab strongly recommends that all Users operating in high-risk environments establish independent emergency communication protocols appropriate to their specific operating environment, entirely separate from the Platform.

6.6 Evidence of acceptance. TraCerLab may record the account, applicable Terms version, acceptance method, and timestamp when a User accepts these Terms or a material update. Those records may be used as evidence of acceptance, subject to applicable law.

6.7 Existing Users - Acceptance of This Version. If you held a Platform account prior to 1 May 2026, you will be prompted to review and confirm acceptance of these Terms at your next login on or after 1 May 2026. Continued access after 1 May 2026 without responding to that prompt constitutes acceptance of these Terms. Acceptance records for both the original registration and this version update are maintained separately in the Platform audit log.

PART V - USER OBLIGATIONS

Article 7 - General Obligations

7.1 You must use the Platform lawfully, honestly, and in good faith. You must not use the Platform in any manner that:

- Violates applicable law or regulation in any relevant jurisdiction
- Infringes the intellectual property rights of TraCerLab or any third party
- Constitutes fraud, misrepresentation, or deception
- Facilitates money laundering, terrorist financing, or sanctions evasion
- Facilitates illegal mineral trade, conflict financing, or child labour
- Violates export control or trade restriction law

7.2 Data Accuracy Obligation. You are responsible for the accuracy and lawfulness of all Client Data. Falsification - including fabricated bag weights, false origin claims, non-existent custody transfers, or forged documents - is a material breach and may constitute a criminal offence. TraCerLab may report suspected falsifications to competent authorities.

7.3 Operational Actor Obligations. Operational Actors must record only events they have personally witnessed or have authority to record; must not fabricate measurements, photographs, or GPS data; and must not record events on

behalf of others without verified authority.

7.4 Compliance Instructions. You must comply with security notices, compliance updates, and operational instructions issued by TraCerLab within the timescales specified.

Article 8 - Data Accuracy and User Responsibility

8.1 Platform outputs depend on the quality, completeness, timing, and context of the information supplied by Users and authorised sources. Instrument readings require suitable equipment and trained operation; manual entries may contain human error; geospatial and registry data may be incomplete, delayed, or inaccurate; and information extracted from documents requires qualified human review before reliance.

8.2 Indemnity for Data Inaccuracy. You agree to indemnify TraCerLab against losses, claims, damages, and regulatory penalties arising from your own submission of inaccurate, fraudulent, or - by reference exclusively to your own acts - unlawfully obtained Client Data. For the avoidance of doubt, "unlawfully obtained" in this clause refers only to data obtained by the User through the User's own unlawful conduct; it does not extend to data received by the User from TraCerLab's own integrations with third parties, including government registries.

PART VI - ACCEPTABLE USE

Article 9 - Permitted Uses

9.1 The Platform is licensed for internal business use by legitimate actors in the mineral supply chain, including mining operations management, field data capture, compliance documentation, KYC/AML workflows, marketplace discovery, government regulatory oversight, and related analytical activities.

9.2 API access is permitted for Partners and Integrators who have executed an API Partner Agreement and operate within the specified rate limits. The applicable API technical documentation, including delivery guarantees, retry limits, and error handling, is published and maintained at: [<https://platform.tracerlabgroup.com/developers/api-docs>] - a specific versioned reference incorporated by reference into these Terms. Where API documentation is updated materially, TraCerLab will notify Partners by email with minimum 14 days' advance notice.

9.3 Government Authorised Users may use the Platform to fulfil oversight, enforcement, and revenue collection mandates subject to the applicable GFA.

Article 10 - Prohibited Conduct

10.1 Absolute Prohibitions:

- Supply Chain Fraud - submitting data that does not accurately reflect physical reality
- KYC Circumvention - submitting false identity documents, impersonating any person or entity, or circumventing sanctions screening
- Platform Security Attacks - denial-of-service attacks, SQL injection, reverse engineering of AI algorithms, circumvention of RLS isolation
- Sanctions Evasion - structuring transactions or documentation to evade applicable sanctions
- Illegal Data Scraping - systematic data extraction by automated means other than TraCerLab-authorized APIs
- Conflict Mineral Laundering - generating false traceability for minerals from conflict areas or armed group mining sites
- Tax Documentation Fraud - fabricating or manipulating calculations for tax evasion purposes
- AI Output Misrepresentation - presenting AI Outputs to any third party as deterministic, authoritative, or government-certified compliance determinations without disclosing their AI-generated and advisory nature
- Unlicensed Sub-licensing - sharing access credentials or API keys with unauthorised parties
- Child Labour Facilitation - documenting supply chain activities involving child labour in breach of applicable ILO standards

10.2 Government Authorised Users must use Platform access only within their official mandate. Extraction of data for non-governmental purposes using regulatory access is prohibited.

10.3 Marketplace Participants must not list minerals without legal title or sale authority; submit false specifications; engage in collusive bidding or price fixing; or use the RFQ system without genuine purchase intent.

PART VII - DATA INTEGRITY AND OWNERSHIP

Article 11 - Client Data - Ownership and Licence

11.1 You retain ownership of all Client Data you submit.

11.2 By submitting Client Data, you grant TraCerLab a limited, non-exclusive, royalty-free licence to host, store, process, analyse, and display your Client Data solely to provide the Services.

11.3 Derived Data. TraCerLab may generate Derived Data by aggregating Client Data and applying measures intended to render it irreversibly anonymous. Derived Data will not identify any individual or specific organisation. TraCerLab may use Derived Data for Platform improvement, AI model development or training, industry benchmark generation, and non-personalised market intelligence only where the information is no longer Personal Data and cannot reasonably be linked to a customer. TraCerLab does not sell identified Client Data. Any commercialisation of Derived Data attributable to a specific customer requires prior written consent under a Data Commercialisation annex.

11.4 AI Training and IP. TraCerLab does not use customer-controlled Personal Data to train a general-purpose model for TraCerLab's own purposes. Where a third-party model provider processes customer-controlled Personal Data on TraCerLab's behalf, TraCerLab will require that provider not to use the data to train a general-purpose model for either party's own purposes. Information that is merely pseudonymised or de-identified but remains reasonably linkable continues to be treated as Personal Data. Irreversibly anonymised information may be used for model evaluation, development, or training. Any materially different use requires an express written agreement, all assessments and lawful bases required by applicable law, and any required notice and choice before the use begins. Nothing in this clause limits a non-waivable data-protection right.

11.5 Government Data. Official government data uploaded by a Government Authorised User remains the sovereign property of the applicable government authority. TraCerLab processes such data exclusively on documented instructions under the GFA and DPA.

Article 12 - Data Integrity Obligations

12.1 You must not submit Client Data that you do not have the legal right to submit. You are responsible for maintaining sufficient backup copies of Client Data critical to your operations.

PART VIII - AI, SCORING, AND ANALYTICAL LIMITATIONS

Article 13 - AI Systems - Advisory-Only Model

13.1 AI components. Depending on the Services and configuration, the Platform may use rules-based, statistical, machine-learning, or other automated components for document processing, identity and restricted-party matching, fraud and anomaly detection, geospatial or scientific analysis, classification, scoring, prediction, assistance, and workflow support.

13.2 All AI Outputs are advisory only. They must always be reviewed by a qualified human decision-maker before use in compliance determinations, regulatory submissions, legal proceedings, or financial decisions. AI Outputs represent the system's probabilistic assessment at the time of processing based on then-available data. They may not reflect subsequent events or information.

13.3 AI governance and applicable law. TraCerLab maintains a risk-based AI governance process designed to identify applicable legal requirements, classify relevant systems and uses, assign human oversight, maintain required documentation and transparency, manage data and performance risks, and review material changes. Where the EU Artificial Intelligence Act or another AI law applies, TraCerLab will comply with the duties applicable to its role and the relevant system or use case.

13.4 Prohibited Reliance. You must not:

- Present AI Outputs as authoritative regulatory determinations without disclosing their AI-generated nature;
- Use AI Outputs as the sole basis for denying any person access to employment, financial services, or other regulated activities;

- Rely on AI Outputs in legal proceedings without independent expert verification.

13.5 Auditability. TraCerLab maintains records of material automated processing and related user or system activity as appropriate to the Service, risk, applicable law, and contractual commitments. Records are retained under the applicable retention schedule and may be disclosed in response to a lawful request.

13.6 Point-of-Reliance Disclosure. TraCerLab undertakes to display a visible advisory notation on all Certificates, Mineral Passports, and AI Output reports delivered by the Platform, in the following form or equivalent: "This document is an advisory output of a technology platform. It does not constitute certification, regulatory approval, or legal proof. See Platform Terms of Use for full limitations." This notation is a contractual commitment applicable to all Platform outputs as of the Effective Date.

13.7 Beta features. A feature identified as beta, preview, pilot, evaluation, or similar is still being assessed and may change, be suspended, or be withdrawn. The applicable Service description or notice identifies material feature-specific limitations.

- SLA: Excluded from all SLA availability and performance commitments
- Liability for Beta Features is governed by Article 26 and the applicable agreement. Beta Features must not be used for production, regulated, safety-critical, or high-impact decisions unless expressly authorised in writing.
- Warranty: Provided without any warranty, express or implied
- Use Restriction: Not to be used for financial projections, regulatory submissions, or commercial commitments

PART IX - TRACEABILITY AND EVIDENCE LIMITATIONS

Article 14 - Nature of Platform Evidence

14.1 Platform Evidence records data as submitted to and processed by the Platform. It does not constitute physical verification.

14.2 Blockchain Anchors provide a cryptographic, time-verified record that a dataset existed at a specific time without subsequent digital modification. They do not verify the accuracy of underlying data, prove that physical events occurred, or substitute for supporting documentation in legal proceedings.

14.3 Evidentiary Value. The potential evidentiary value of Platform Evidence in any legal or regulatory proceeding is determined by applicable rules of evidence in that proceeding. TraCerLab makes no representation about admissibility or weight in any jurisdiction. Users relying on Platform Evidence in legal proceedings must obtain independent legal advice.

14.4 Reconstructibility. Audit logging, AI prompt trails, and blockchain anchoring support forensic reconstruction of Platform activities. The Public Track & Verify feature permits external verification of anchored records without Platform login. TraCerLab will cooperate with lawful requests for audit log production subject to applicable law.

14.5 Data Retention for Non-MSA Users. If you do not hold a signed MSA, the following minimum retention periods apply to your Client Data:

Data Category	Minimum Retention	Legal Basis
Account and identity data	Duration of account + 2 years	Contract performance; legal obligation
KYC and compliance records	5 years post-relationship end	AML/CFT legal obligation
Traceability records (bags, batches, custody, exports)	5 years from creation	Legal obligation; audit requirement
Financial transaction records	7 years	Tax and accounting legal obligation
AI Output logs and prompt audit trails	5 years	Forensic audit; legal obligation
Blockchain Anchor records	Indefinite (blockchain-native)	Immutable ledger

Full retention schedules for MSA holders are set out in Annex Doc 8 of the MSA and the applicable Exit/Transition Plan (Annex Doc 31).

PART X - KYC, IDENTITY, AND DOCUMENT PROCESSING

Article 15 - KYC Processing

15.1 KYC and identity verification functions are designed to assist Users in their own compliance workflows. The Platform's KYC engine is a technology tool - it is not an AML-regulated institution performing KYC as a compliance service on behalf of Users.

15.2 KYC Output Limitations. Automated verification results are advisory, subject to error, and not a substitute for required human review in regulated AML/CFT workflows.

15.3 Sanctions-screening limitations. Where enabled, screening may use public, internal, customer-authorised, or licensed data sources. Coverage, refresh frequency, matching logic, and source quality may vary. Screening outputs are advisory and may contain false positives, false negatives, or incomplete information. Users remain responsible for selecting appropriate screening sources, reviewing potential matches, and meeting their own AML and sanctions obligations.

15.4 Identity Document OCR. OCR accuracy depends on document quality and type. Human review of OCR-extracted data is required before use in compliance records.

15.5 Biometric and identity features. A feature-specific notice will identify any biometric or automated identity-comparison processing before it is enabled for a User. Such processing will be subject to the applicable agreement, a documented lawful basis and any additional sensitive-data condition, required notices or consent, and appropriate human review and safeguards.

Article 16 - KYB and Entity Verification

16.1 KYB and entity-verification functions may use documents, official or commercial registries, customer-authorised sources, and specialist service providers. Outputs are advisory and may be incomplete or outdated. Users responsible for regulated onboarding must complete any additional checks required by law and their own risk-based procedures.

PART XI - MARKETPLACE

Article 17 - TraCerLab MARKET - Terms and Limitations

17.1 Nature of Marketplace. TraCerLab MARKET is a B2B technology intermediary. TraCerLab is not a party to any trade transaction negotiated therein.

17.2 Deal workflow. The Marketplace may support configurable transaction stages. A stage displayed in the Platform does not mean that TraCerLab provides the underlying regulated, banking, payment, settlement, escrow, logistics, or inspection service. Any such service is governed by the applicable agreement and the terms of the relevant authorised provider.

17.3 Marketplace Data - Joint Controller Arrangement. When TraCerLab processes Marketplace Participant transaction data for platform safety, fraud detection, and legal compliance purposes, TraCerLab and the relevant Marketplace Participants may each be Data Controllers for overlapping sets of personal data. In accordance with GDPR Article 26:

- TraCerLab acts as an independent Data Controller for its own platform safety and fraud detection processing;
- Where TraCerLab's processing of one Participant's data involves another Participant's personal data, TraCerLab and the relevant Parties are Joint Controllers for that processing;
- TraCerLab is responsible for responding to Data Subject Requests from Marketplace Participants relating to data processed primarily in the marketplace context. Where a DSAR cannot be fulfilled without the assistance of the counterparty Controller, TraCerLab will coordinate that response within the timeframes required by GDPR;
- This arrangement is set out in the Marketplace Data Processing Annex, available on request and automatically incorporated into any signed Marketplace participation agreement.

17.4 Listing Accuracy. Sellers are solely responsible for the accuracy of all listing data. Buyers are entitled to rely on material listing representations. Sellers are liable to buyers for material misrepresentation.

17.5 Trade Compliance. Marketplace Participants bear sole responsibility for ensuring transaction compliance with applicable export, sanctions, customs, and AML law.

17.6 Platform Neutrality. TraCerLab does not endorse or warrant any Participant, listing, or transaction. Commercial disputes are between the transacting parties.

PART XII - COMMUNICATIONS

Article 18 - Communications Services

18.1 SMS. Where enabled, SMS is delivered through communications service providers and mobile networks. Delivery may be delayed or fail because of coverage, routing, filtering, device, recipient, or provider conditions.

18.2 SMS Attestations. SMS-submitted attestations through designated workflows are logged as binding declarations. Organisations authorising SMS attestation workflows are responsible for ensuring attesting individuals have authority and intention to make the transmitted declarations.

18.3 Email. Automated email notifications depend on delivery infrastructure and recipient spam filters. Not guaranteed.

18.4 Messaging integrations. A messaging integration is included only if it is identified as available in the applicable Service description or Order Form. Users must comply with the relevant channel rules and must not rely on a messaging integration for emergency communications.

18.5 Webhooks. Event-driven webhook notifications are available to Partners and Integrators. Delivery behaviour, retry limits, failure notifications, and SLA parameters are specified in the API Technical Documentation at: [<https://platform.tracerlabgroup.com/developers/api-docs>]. TraCerLab does not guarantee webhook delivery in the event of recipient endpoint unavailability beyond the retry parameters specified therein.

18.6 No Emergency Use. The Platform is not an emergency communications system. No Platform element should be used to communicate in life-threatening situations or to contact emergency services.

PART XIII - THIRD-PARTY DEPENDENCIES

Article 19 - Third-Party Services

19.1 The Platform uses third-party technology and data services, which may include hosting, identity, communications, mapping, document processing, analytics, distributed-ledger, payment, registry, and support services. The categories used for a particular Service may change as the Platform develops.

19.2 Supplier management. TraCerLab selects and oversees material service providers using risk-based due diligence, contractual controls, security requirements, continuity planning, and performance monitoring appropriate to the service and information involved. A third-party disruption may nevertheless affect a Service. Responsibility and any remedy are determined by the applicable agreement, SLA, these Terms, and mandatory law.

19.3 Supplier transparency. TraCerLab maintains a current Subprocessor and Transfer Register identifying each relevant provider, function, processing location, and transfer mechanism where required. Applicable register information and change notices are provided in accordance with the Data Processing Agreement and applicable law.

19.4 External data. Satellite, mapping, registry, sanctions, identity, and other external data may be incomplete, delayed, unavailable, or affected by source methodology and conditions. Such data is indicative and must be independently verified before use in a regulatory, enforcement, financial, or other significant decision.

19.5 Government and registry data. TraCerLab does not warrant that an external registry is complete, current, or error-free. A Platform connection to a public or customer-authorised source does not imply endorsement or a formal relationship with the source authority. Discrepancies must be resolved by reference to the competent authority or authoritative source.

PART XIV - SERVICE AVAILABILITY

Article 20 - Availability

20.1 Service levels. Availability commitments, maintenance windows, recovery objectives, support response times, service credits, and exclusions apply only where stated in the applicable Order Form, Service Level Agreement, Government Framework Agreement, or Master Services Agreement.

20.2 Operational resilience. TraCerLab maintains business-continuity and disaster-recovery arrangements proportionate to the nature and risk of the Services. These arrangements are reviewed and tested at intervals determined through TraCerLab's risk-management programme.

20.3 Recovery. Recovery priorities and objectives are set according to service criticality and may be described in the applicable service or security schedule. An objective is a planning measure and is not a guarantee unless expressly stated in a signed agreement.

20.4 Service-level exclusions. Any exclusions from service-level commitments, including events beyond reasonable control, are governed by the applicable SLA and Article 28.

20.5 Offline capability. Offline functionality varies by module, device, configuration, and workflow. Customers requiring offline operation or synchronisation must confirm the relevant requirements and acceptance criteria in the applicable agreement before deployment.

20.6 Service information. TraCerLab may publish current service-status and incident information through its designated status channel.

PART XV - SECURITY

Article 21 - Security Controls

21.1 Security programme. TraCerLab maintains risk-based administrative, technical, and organisational safeguards designed to protect the confidentiality, integrity, availability, and resilience of the Services and Personal Data. Measures may include encryption, access control, multi-factor authentication, logging, monitoring, secure development, vulnerability management, backup, recovery, incident response, supplier controls, and personnel measures, as appropriate to the relevant risk.

21.2 Security assurance and testing. TraCerLab reviews its security programme regularly and performs risk-based internal and external assessment activities, which may include vulnerability assessment, penetration testing, control testing, supplier assurance, and independent audits. The scope and frequency reflect the Services, applicable law, contractual commitments, risk, and material changes. Current assurance information may be provided through a security questionnaire or confidential due-diligence process. Nothing in these Terms represents that TraCerLab holds a particular certification unless expressly confirmed in current written assurance material.

21.3 Incident response. TraCerLab maintains documented incident-response procedures and reviews them at intervals determined through its security programme. Applicable incident-response commitments are stated in the Data Processing Agreement or security schedule and may be supported through customer due diligence.

21.4 User Security Obligations. You are responsible for: credential security; not sharing credentials with unauthorised persons; promptly reporting suspected security incidents to security@tracerlabgroup.com; securing local devices used to access the Platform; securing all webhook and API integration endpoints.

21.5 Incident notification. TraCerLab will notify affected customers of a confirmed Personal Data breach within the period and with the information required by the applicable Data Processing Agreement and data-protection law.

PART XVI - DATA HANDLING

Article 22 - Data Protection

22.1 Privacy Policy. TraCerLab's Privacy Policy - published and maintained at [\[https://platform.tracerlabgroup.com/legal/privacy-policy\]](https://platform.tracerlabgroup.com/legal/privacy-policy) - describes how Personal Data is collected, used, stored, transferred, and how data subject rights may be exercised. It is incorporated into these Terms by reference. It is published in English and French and will be published in additional languages as required per the Offline Consent framework (POL-EN-002).

22.2 Data Processing Roles:

- Processor: In respect of Client Data containing Personal Data, TraCerLab acts as Data Processor processing on behalf of the User as Data Controller, under the DPA.
- Independent Controller: For data TraCerLab processes for its own purposes (platform security, fraud detection, Derived Data analytics), TraCerLab acts as an independent Data Controller.
- Joint Controller: In marketplace data processing contexts, as described in Article 17.3.
- Government Deployments: Specific data role arrangements are defined in the applicable GFA and DPA.

22.3 GDPR. TraCerLab is incorporated in Belgium and is directly subject to GDPR as a Data Processor under Article 28. Users acting as Data Controllers are responsible for ensuring their own instructions to TraCerLab are lawful and their own processing complies with GDPR.

22.4 United States privacy. Where applicable United States state privacy law applies, TraCerLab provides the rights and disclosures described in the Privacy Policy. TraCerLab does not sell Personal Data or share it for cross-context behavioural advertising as those terms are defined by applicable law. International transfers involving service providers are governed by the safeguards described in Article 22.5.

22.5 International Transfers. Personal Data transferred outside the EEA is covered by an applicable adequacy decision or another lawful mechanism for the actual transfer and roles, including the European Commission's Standard Contractual Clauses, the EU-US Data Privacy Framework for eligible and actively certified recipients, and transfer assessments with supplementary measures where required. Provider, function, processing-location, and transfer-mechanism details are maintained in TraCerLab's current Sub-Processor and Transfer Register and, where applicable, the Sub-Processors Annex (Doc 16 of the MSA).

22.6 Data-subject requests. TraCerLab handles requests in accordance with its role, applicable law, the Privacy Policy, and the Data Processing Agreement. Where TraCerLab acts as processor, it assists the relevant customer and follows documented instructions, subject to legal obligations and permitted exceptions.

22.7 Privacy contact. Privacy enquiries and requests may be sent to privacy@tracerlabgroup.com. Where applicable law requires a data-protection officer, representative, or other designated contact, the relevant notice will provide the current details.

PART XVII - INTELLECTUAL PROPERTY

Article 23 - Ownership

23.1 TraCerLab IP. TraCerLab owns all intellectual property rights in: the Platform software, architecture, and source code; AI models and algorithms, including the Geochemical Rosetta Engine and Mineral DNA fingerprinting methodology; the Innovation Lens framework; and all Platform documentation and visual design.

23.2 Protected methods and know-how. Platform methods, models, workflows, documentation, and technical designs may be protected by copyright, database rights, patent rights, or trade-secret law. No right to reverse engineer, reproduce, or commercially exploit them is granted except where a signed agreement or mandatory law expressly permits it.

23.3 Client Data. You retain all IP rights in Client Data. Nothing transfers ownership to TraCerLab.

23.4 Feedback. You grant TraCerLab an irrevocable, royalty-free licence to implement any feedback or suggestions you provide.

23.5 Platform Licence. TraCerLab grants you a limited, non-exclusive, non-transferable, non-sublicensable, revocable licence to access and use the Platform solely for the permitted purposes in these Terms and any applicable Order Form.

PART XVIII - SUSPENSION AND TERMINATION

Article 24 - Suspension

24.1 TraCerLab may suspend access immediately, without prior notice, where:

- Reasonable grounds exist to suspect material breach including fraud or data falsification
- A security threat or active attack is detected

- A confirmed sanctions list match is identified following manual review (see 24.2)
- Undisputed Fees remain unpaid beyond 30 days
- Legal proceedings create material risk to the Platform or other Users

24.2 Automated sanctions match review. Where access is restricted because of a potential automated sanctions match, TraCerLab will provide notice where legally permitted, conduct qualified human review, allow the User a reasonable opportunity to provide relevant information, and communicate the outcome and available challenge route. A temporary restriction does not determine that the User is sanctioned.

24.3 Marketplace Suspension. TraCerLab may suspend a Marketplace Participant's ability to list, offer, or accept deals pending investigation of suspected fraudulent or non-compliant conduct, with notice where operationally practicable.

Article 25 - Termination

25.1 For Cause. TraCerLab may terminate immediately for: confirmed material breach not remedied within 14 days of notice (or immediately where the breach is incapable of remedy); confirmed sanctioned person or entity status following the Article 24.2 procedure; or fraudulent Platform use.

25.2 For Convenience. Users may terminate at any time through the account management interface.

25.3 Effects. On termination: Platform access ceases immediately; Client Data is retained for the periods in Article 14.5 (non-MSA) or Annex Doc 8 (MSA holders), then securely deleted or returned; outstanding payment obligations survive; provisions that by their nature survive termination remain in force.

PART XIX - LIABILITY

Article 26 - Limitation of Liability

26.1 Contractual allocation of liability. Monetary liability caps and any account-specific allocation of risk are agreed in the applicable Order Form, Master Services Agreement, Government Framework Agreement, or other signed contract. These Terms do not state a monetary liability cap. Where no signed agreement addresses liability, liability is determined under applicable law, subject to the provisions of this Article that may lawfully apply.

Any contractual liability cap remains subject to the mandatory exceptions in Article 26.6.

26.2 Exclusion of Indirect Damages. To the maximum extent permitted by law, TraCerLab shall not be liable for:

- Loss of profit, revenue, or business opportunity
- Loss of data (beyond the obligation to restore from backup under TraCerLab's control)
- Loss of goodwill or reputational damage
- Regulatory fines or penalties imposed on you by any authority
- Indirect, consequential, exemplary, special, or punitive damages
- Third-party claims against you based on your use of Platform Evidence

26.3 Reliance Exclusion. TraCerLab shall not be liable for loss arising from your reliance on any AI Output, Platform Evidence, or Beta Feature output without the independent human review required by these Terms.

26.4 Third-party services. To the extent permitted by law and the applicable agreement, TraCerLab is not responsible for a third-party service failure that is outside its reasonable control. This does not exclude responsibility that arises from TraCerLab's own breach of an applicable duty concerning supplier selection, contracting, oversight, security, continuity, or incident response.

26.5 Scientific Uncertainty Exclusion. TraCerLab is not liable for loss arising from the inherent statistical uncertainty of geochemical provenance matching, XRF analysis, or AI-generated classification, provided outputs are used consistently with the advisory-only requirements of these Terms and the uncertainty parameters published in the Technical Methodology Documents.

26.6 Mandatory Exceptions. Nothing in these Terms limits or excludes liability:

- For death or personal injury caused by TraCerLab's negligence
- For fraud or fraudulent misrepresentation by TraCerLab

- For any liability that cannot be excluded by Belgian law
- For any other unexcludable mandatory statutory liability

26.7 Consumer Rights. If, notwithstanding Article 5.1, you qualify as a consumer under applicable law, your mandatory consumer protection rights are unaffected by these Terms.

PART XX - INDEMNIFICATION

Article 27 - Indemnification

27.1 Your Indemnity. You shall indemnify, defend, and hold harmless TraCerLab, its directors, employees, agents, and sub-processors from all third-party claims, liabilities, damages, and costs (including legal costs) arising from:

- Your material breach of these Terms
- Client Data submitted by you that infringes third-party IP rights
- Your submission of inaccurate or fraudulent Client Data, or Client Data that you obtained through your own unlawful conduct
- Your violation of applicable law, including AML/CFT, export control, or sanctions law
- Any transaction or dispute between you and any other Marketplace Participant
- Any third-party claim arising from a compliance determination you made on the basis of Platform Evidence without conducting the human review required by these Terms, where TraCerLab can demonstrate that the human review requirement was communicated to you and you deliberately or recklessly bypassed it

27.2 TraCerLab Indemnity. TraCerLab shall indemnify you against third-party claims that the Services, as provided and used in accordance with these Terms, infringe any third-party copyright, patent, or trade secret, subject to the liability cap in Article 26.

PART XXI - FORCE MAJEURE

Article 28 - Force Majeure

28.1 Neither party is liable for failure or delay in performance to the extent caused by events beyond their reasonable control, including: natural disasters; acts of war, terrorism, or civil unrest; acts or failures of government authorities; failures of public internet or telecommunications infrastructure; and blockchain network failures or protocol changes.

28.2 Third-party events. A failure of a supplier, network, authority, registry, or external infrastructure may constitute a force majeure event only to the extent it is beyond the affected party's reasonable control and could not reasonably have been prevented or overcome. Any effect on service levels or remedies is determined under the applicable SLA and mandatory law.

28.3 The affected party shall notify the other promptly and use reasonable efforts to mitigate. If the force majeure event continues beyond 60 days, either party may terminate the affected Services on written notice.

28.4 SLA interaction. The treatment of a force majeure event under a service-level commitment is governed by the applicable SLA. Nothing in this Article creates an exclusion broader than the applicable agreement or mandatory law permits.

PART XXII - EXPORT CONTROL AND SANCTIONS

Article 29 - Export Controls

29.1 You must comply with all applicable export control and sanctions laws, including EU and UK export control regulations, US EAR, and ITAR where applicable.

29.2 The Platform must not be used to facilitate the export or transfer of activities requiring export licences without first obtaining those licences.

29.3 You confirm you are not located in, incorporated in, or acting on behalf of any government of a jurisdiction currently subject to comprehensive sanctions enforced by the EU, US, UK, or UN.

29.4 You must notify TraCerLab immediately of any suspected sanctions evasion conducted through or related to the Platform.

PART XXIII - GOVERNMENT AND PUBLIC-SECTOR

Article 30 - Government Use

30.1 Precedence. For Government Authorised Users under a GFA, the GFA governs to the extent of any conflict. These Terms apply concurrently for all matters not addressed by the GFA.

30.2 Sovereign Data. Government data remains the sovereign property of the applicable authority. TraCerLab processes it exclusively on documented instructions under the GFA and DPA. TraCerLab will honour lawful government directives on data access, retention, or disclosure in accordance with applicable law.

30.3 Enforcement - Advisory Outputs. As stated in Article 3.10, Platform outputs used in enforcement contexts are evidentiary indicators requiring independent human expert review. TraCerLab's involvement does not constitute expert testimony or official certification unless separately agreed in writing.

30.4 Lawful Access. TraCerLab may be required by law to provide access to Platform records to competent authorities without prior notice. TraCerLab will assert available legal protections before complying and will notify the affected User where legally permissible.

30.5 Jurisdiction Conflicts. Where applicable law in a government User's jurisdiction conflicts with Belgian law, TraCerLab and the counterparty shall cooperate to identify a compliant arrangement. Where no compliant arrangement is achievable, TraCerLab may decline to provide the affected Services.

30.6 No Delegated Public Authority. TraCerLab does not exercise delegated public authority, regulatory power, or law enforcement function. No Platform output constitutes an administrative decision binding on any person under public law.

PART XXIV - DISPUTE RESOLUTION

Article 31 - Dispute Resolution and Governing Law

31.1 Informal Resolution. Parties shall use good-faith negotiations for 30 days before formal escalation.

31.2 Signed Agreements. Where a signed MSA or GFA exists, its dispute resolution provisions apply and supersede this Article.

31.3 Standard User disputes - arbitration. For disputes not subject to a signed MSA or GFA, and not subject to the consumer carve-out in Article 5.2, any dispute arising out of these Terms shall be resolved by final, binding international arbitration under the ICC Rules, seated in Brussels, Belgium, and conducted in English. The number and appointment of arbitrators are determined under the applicable rules unless the parties agree otherwise in writing.

31.4 Consumer Users. If you qualify as a consumer under applicable law, you may choose to resolve disputes before the competent courts of your place of residence or the courts of Brussels, at your election, and the arbitration clause in Article 31.3 does not apply to you.

31.5 Class Action Waiver. To the maximum extent permitted by applicable law, all disputes must be brought on an individual basis. You waive any right to participate in a class, collective, consolidated, or representative arbitration or litigation proceeding. This waiver does not apply to users who qualify as consumers under applicable law.

31.6 African Operations - OHADA. For Users whose Organisational Account is registered and whose operations giving rise to the dispute are located in an OHADA member state (including DRC and Mauritania), and in respect of commercial disputes arising from supply chain, tax, or marketplace activities under those operations:

- Arbitration shall be conducted under the OHADA Uniform Act on Arbitration Law;
- The arbitral institution shall be the Common Court of Justice and Arbitration (CCJA), seated in Abidjan, Ivory Coast, and its Arbitration Rules shall govern;
- The seat of arbitration shall be Abidjan unless the parties agree otherwise in a signed Country Supplement;

- This OHADA provision is an operative arbitration clause affecting the selection of institution, rules, and seat - it is not simply a general cross-reference.

31.7 Governing Law. These Terms are governed by Belgian law, excluding conflict-of-law rules. The CISG does not apply.

31.8 Regulatory Authority Jurisdiction. Nothing limits the jurisdiction of any competent supervisory authority (including the Belgian Data Protection Authority and equivalent EU DPAs) over matters within their regulatory mandate.

31.9 Interim Relief. Either party may seek interim or injunctive relief from courts in any jurisdiction necessary to prevent irreparable harm, notwithstanding the arbitration clause.

31.10 US Jurisdiction Addendum. For Organisational Accounts incorporated or primarily operating in the United States:

- US enterprise accounts may request a US Law Addendum setting out applicable governing law election and forum for US operations;
- The class action waiver in Article 31.5 is specifically intended to comply with US arbitration law requirements and is severable from the remainder of this Article if held unenforceable in any US proceeding;
- For purposes of CCPA/CPRA compliance, TraCerLab's designated representative for California privacy matters is reachable at privacy@tracerlabgroup.com.

PART XXV - VERSIONING AND CHANGE MANAGEMENT

Article 32 - Term Changes

32.1 Version control. Each published version of these Terms is identified by document identifier, version number, and effective date. TraCerLab retains prior versions as required for legal, contractual, audit, and evidence purposes.

32.2 Change Classification:

Type	Examples	Notice	Re-Acceptance
Material	Material changes to liability allocation, prohibited uses, privacy rights, or data-processing purposes	30 days advance	Required - in-platform prompt at next login
Non-Material	Clarifications; typographical corrections; new defined terms for existing concepts	14 days	Not required
Regulatory-Driven	Changes required by new legislation or regulatory guidance	As soon as practicable	As required by the change
Emergency	Critical security or legal compliance	Immediate; retrospective notice within 5 days	Confirmatory re-acceptance within 30 days

32.3 Notice. Material change notices are sent to Organisational Account administrator email addresses and displayed as in-Platform notifications.

32.4 Existing Users. Existing users at the date of a material change are prompted to affirmatively accept at next login. Continued access after the acceptance prompt without responding constitutes acceptance.

32.5 Signed Agreements. Material changes to these Terms do not automatically modify signed MSA or GFA terms. Changes to signed contracts require mutual written agreement.

CONTACT

Purpose	Contact
General legal	legal@tracerlabgroup.com

Purpose	Contact
Data protection / privacy	privacy@tracerlabgroup.com
Security incidents	security@tracerlabgroup.com
Marketplace disputes	marketplace@tracerlabgroup.com
Regulatory / government	government@tracerlabgroup.com
US / California privacy	privacy@tracerlabgroup.com - California Privacy Rights
Registered office	TraCerLab SC, Avenue Marcel Gourdin 60, 5001 Namur, Belgium; VAT BE0758359658 www.tracerlabgroup.com

Document: Version: 4.0 | Effective: 1 May 2026 This document is reviewed periodically and following material changes to the Services, applicable law, or commercial arrangements.