

Global Privacy Policy and Data Protection Notice

Document control	Details
Version	3.0
Effective Date	1 September 2026
Last Updated	1 October 2026
Supersedes	Version 2.0
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
Privacy Contact	privacy@tracerlabgroup.com
Classification	Public - client-facing

1. Purpose, legal effect, and scope

This Privacy Policy and Data Protection Notice (the "Policy") explains how TraCerLab collects, obtains, uses, generates, discloses, transfers, stores, retains, and deletes information relating to an identified or identifiable natural person ("Personal Data"). Where applicable law protects information relating to a household or affords equivalent protection to another category of information, references to Personal Data include that protected information. This Policy also explains the choices and rights available to individuals.

This Policy applies to TraCerLab's websites, software, services, features, support, and other current or future offerings that link to or expressly incorporate this Policy (collectively, the "Services"). The Personal Data processed depends on the Service and feature used, the account configuration, the relevant customer instructions, and the individual's relationship with TraCerLab.

A separate or supplemental notice may apply to a particular Service, feature, collection point, processing activity, deployment, or jurisdiction. The more specific notice applies to the activity it describes if it conflicts with this Policy. Adding or renaming a Service does not authorise TraCerLab to collect a materially new category of Personal Data or use Personal Data for a materially new purpose without giving any additional notice or obtaining any choice required by law before that processing begins.

This Policy sets out TraCerLab's public privacy commitments from the Effective Date. Where an agreement expressly incorporates it, it also forms part of that agreement. It does not replace a data processing agreement ("DPA"), transfer controller obligations to a processor, create a lawful basis that does not otherwise exist, or require an individual to waive a non-waivable right. Merely visiting or using a Service is not consent to processing. Where consent is required, TraCerLab requests it separately through a clear affirmative choice.

The Services are intended for business, professional, institutional, research, and governmental use by adults. Privacy and consumer-protection laws may nevertheless protect an individual acting in a professional capacity.

1.1 Who this Policy covers

This Policy may apply to:

- visitors to a TraCerLab website, public page, documentation page, or verification interface;
- prospective, current, and former customers and their personnel;
- account administrators, authorised users, field or operational users, partner and integration personnel, and public officials;
- suppliers, contractors, advisers, and other business contacts;
- individuals identified in records, documents, communications, evidence, or other content submitted through the Services by a customer or authorised user;
- individuals involved in identity, due-diligence, counterparty, transaction, safety, incident, ethics, or compliance workflows;
- people who contact support, request information, attend an event, submit feedback, make a privacy request, or report a concern; and
- job applicants who apply through a TraCerLab-controlled channel, unless a separate applicant notice is provided.

1.2 What this Policy does not cover

This Policy does not govern:

- an independent third party's website, application, network, or service, even if linked from a Service;
- a customer's independent use of Personal Data outside the Services;
- workforce processing governed by a separate employee or contractor notice; or
- information that has been irreversibly anonymised so that no person is identifiable by means reasonably likely to be used.

Pseudonymised, hashed, or otherwise de-identified information remains Personal Data when it can reasonably be linked back to a person.

2. At-a-glance notice

Topic	Summary
Who is responsible	TraCerLab is a controller for its own websites, business relationships, account administration, billing, support, security, legal compliance, communications, and other purposes it determines. It is ordinarily a processor for Personal Data a customer controls and submits to the Services.
What we process	Depending on context: identity and business contact data; account and authentication data; customer-submitted content; identity and compliance documents; operational, transaction, location, safety, communications, device, usage, log, integration, and AI-related data.
Why	To operate and secure the Services; manage accounts and business relationships; follow customer instructions; provide support; prevent abuse and fraud; meet legal duties; communicate; improve performance; and provide configured analytics or AI-assisted functionality.
Sensitive data	Certain configured workflows may involve official identifiers, precise location, photographs, due-diligence information, safety information, or other sensitive data. Additional safeguards and a valid legal condition are required.
Sale and targeted advertising	TraCerLab does not sell Personal Data or use it for third-party targeted advertising.
General AI training	Customer-controlled Personal Data is not used to train a general-purpose model for TraCerLab's own purposes. TraCerLab requires third-party model providers acting on its behalf to observe the same restriction. Information that has first been irreversibly anonymised is no longer Personal Data and may be used for service evaluation and improvement.
International processing	Personal Data may be processed in countries other than the country where it was collected. TraCerLab uses a lawful transfer mechanism where one is required.
Retention	Retention depends on TraCerLab's role, the data type, customer instructions, the applicable agreement and law, and documented security, evidence, or legal-claim needs. Any approved fixed period is stated in the applicable retention schedule or collection-point notice.

Topic	Summary
Your rights	Depending on applicable law: information, access, correction, deletion, restriction, portability, objection, consent withdrawal, appeal, and safeguards for significant automated decisions.
How to contact us	Email privacy@tracerlabgroup.com . If TraCerLab processes the data only for a customer, the customer is normally the appropriate controller to contact.

3. Our data-protection roles

Our role is determined by the actual processing activity and who determines its purposes and essential means, not by a product name or contractual label.

Context	TraCerLab's usual role	What this means
Websites, enquiries, sales, events, business contacts, account administration, billing, support-case administration, service security, fraud prevention, legal compliance, and TraCerLab's own communications	Controller	TraCerLab determines why and how the Personal Data is processed and is responsible for the controller duties described in this Policy. Customer content included in a support case remains processor data where TraCerLab handles it only to assist the customer.
Content and records that a customer submits, imports, captures, or makes available through the Services for purposes determined by that customer	Processor / service provider / contractor	The customer is the controller or business and TraCerLab processes the Personal Data on documented instructions under the applicable DPA or equivalent terms. The customer determines the lawful basis, required notices, permitted data, and retention or deletion instructions, except where applicable law or the DPA requires otherwise.
Service-integrity, abuse-prevention, security, and legal-compliance processing that TraCerLab determines independently even when it relates to a customer account	Independent controller	TraCerLab is responsible for its own defined purposes. It does not become controller of all underlying customer content merely because it secures or processes it.
A limited activity for which TraCerLab and another organisation genuinely determine the purposes and essential means together	Joint controller, only where the legal test is met	The parties use a written allocation of responsibilities and make the essence of that arrangement available through a specific notice or on request. Providing a shared technical environment does not by itself create joint control.
Irreversibly anonymised statistics or aggregates	Not Personal Data	TraCerLab may use them for service improvement, research, benchmarking, security analysis, and business intelligence, but will not attempt to re-identify individuals.

If Personal Data about you was submitted by a customer, employer, public authority, research institution, or other organisation that controls it, consult that organisation's privacy notice and direct your request to it. TraCerLab will forward or assist with the request as required by law and contract. Nothing in this section prevents you from contacting TraCerLab, and nothing changes a role assigned by mandatory law.

4. Personal Data we may process

Not every category is collected about every person. Collection depends on the relevant relationship, Service, feature, configuration, and customer instructions.

Category	Examples
Identity, contact, and professional data	Name, title, signature, business email, telephone number, preferred language, organisation, department, role, professional profile, and business address.

Category	Examples
Account, authentication, and permission data	User and account identifiers, username, password verifier, authentication and recovery data, organisation membership, permissions, access role, session data, acceptance record, and account status.
Contract, subscription, billing, and commercial data	Order and contract details, subscription or entitlement, invoicing and billing contact data, tax and accounting information, payment status, limited payment metadata, and transaction history, where relevant.
Customer-submitted content and service records	Forms, documents, project and case records, workflow data, permits, licences, certificates, reports, evidence, transaction or supply-chain records, chain-of-custody events, quantities, comments, annotations, and any Personal Data contained in uploaded or integrated content.
Identity, due-diligence, and compliance data	Date of birth, nationality or citizenship, official identifier and document, proof of address, photograph, licence or permit, beneficial-owner or director information, entity affiliation, verification result, restricted-party match, review note, and challenge evidence, where the relevant workflow is enabled.
Location, operational, workforce, and safety data	Precise or approximate coordinates, site or route location, timestamps, field activity, assignment or shift information, device location, check-in, safety or duress alert, incident record, exposure or health-and-safety information, and associated metadata, where configured and lawfully authorised.
Communications and support data	Emails, contact forms, support tickets, in-service messages, survey and feedback responses, notification choices, and, where enabled, electronic message content and routing, delivery, and timestamp metadata. A recording is made only with required notice or permission.
Device, network, cookie, and usage data	IP address, browser, operating system, device type, language, time zone, session and cookie identifiers, security-oriented device signals, pages and functions used, interaction events, referral information, approximate location derived from network information, error and performance telemetry, and consent records.
Audit, integrity, and security data	Login attempts, user and administrator actions, access and change logs, system events, timestamps, security alerts, suspected abuse or policy violations, incident evidence, and integrity records.
Integration and delivery data	Integration identifiers, connection and event data, imported and exported records, delivery and error metadata, and the identity of the initiating user or system.
AI, analytics, and inferred data	Prompts, queries, source inputs, extracted text, system or ruleset version, outputs, classifications, confidence or anomaly scores, flags, predictions, explanations, user feedback or override, and accountability metadata. A score or flag may be Personal Data when it relates to a person.
Image, audio, video, and document data	Photographs, identity-document images, scans, site or evidence images, signatures, audio, and video submitted through an enabled feature.
Public-source and third-party data	Information from official registries, public authorities, regulatory lists, professional sources, customer-authorised providers, data partners, maps, geospatial sources, counterparties, and publicly accessible sources.
Recruitment and supplier data	CV, employment history, qualifications, references, interview notes, eligibility data, conflicts, supplier due-diligence data, and professional contact details.
Ethics, complaints, requests, and legal data	Privacy requests and verification, complaints, whistleblowing or ethics reports, allegations, witness or investigation material, dispute and claim records, legal holds, authority requests, and related correspondence.
Preferences and consent records	Marketing, notification, cookie, privacy, and feature choices; date, time, method, language, notice version, withdrawal, and related proof.

4.1 Sensitive, special-category, and criminal-offence data

Some data above can be sensitive under applicable law, including official identifiers, account credentials, precise location, citizenship or immigration status, communications content, photographs used for unique identification, health or exposure data, and information revealing protected characteristics.

When TraCerLab acts as controller and processes special-category data under Article 9 GDPR or UK GDPR, it will identify both an Article 6 lawful basis and an applicable Article 9 condition, such as explicit consent, employment or social-protection law, protection of vital interests, establishment or defence of legal claims, or substantial public

interest grounded in applicable law. TraCerLab will process criminal-conviction or offence data under Article 10 only under official authority or where authorised by applicable law with appropriate safeguards.

When TraCerLab acts as processor, the customer must identify and document the applicable legal conditions, give required notices, and configure appropriate safeguards. Users must not submit sensitive data unless the relevant feature, customer instruction, and law permit it.

A photograph is not biometric data under the GDPR merely because it depicts a person; it becomes biometric data when specific technical processing is used to uniquely identify that person. TraCerLab will not introduce that processing without completing the legally required assessment, giving a specific notice, establishing a lawful condition, and obtaining explicit consent where consent is the applicable condition.

5. Where Personal Data comes from

TraCerLab may obtain Personal Data:

- Directly from you, including through a website, account, form, upload, communication, support request, consent flow, event, application, or use of a Service.
- From a customer or its authorised users, including your employer, contracting organisation, public authority, institution, account administrator, field operator, or another participant in a configured workflow.
- From your device and use of the Services, including cookies, local storage, network requests, audit logs, telemetry, and security signals.
- From integrations and service providers, including identity, communications, payment, mapping, security, support, and customer-authorised systems.
- From public and official sources, including corporate and professional registries, public records, regulatory lists, government sources, and websites lawfully accessed for verification.
- From counterparties, partners, advisers, and other third parties where they are authorised to provide the data.
- By generation or inference, including risk, anomaly, similarity, confidence, classification, integrity, or workflow signals derived from source data.

Where TraCerLab acts as controller and receives Personal Data from another source, it provides the information required by applicable law within the required period, ordinarily no later than one month under the GDPR, or at the first communication or disclosure if earlier, unless a documented legal exception applies. Public availability does not by itself remove TraCerLab's data-protection obligations.

6. Why we process Personal Data and our lawful bases

The following table applies when TraCerLab acts as controller under the GDPR or UK GDPR. More than one basis may apply to different elements of an activity. TraCerLab documents the applicable basis in context and does not rely on a customer's legal basis for its own independent purpose.

Activity and purpose	TraCerLab role	GDPR / UK GDPR basis when TraCerLab is controller
Operate websites; respond to enquiries, demonstrations, proposals, and requested support	Controller	Steps requested before a contract or performance of a contract with the individual, where applicable; otherwise legitimate interests in responding and operating our business.
Create and administer accounts, permissions, authentication, entitlements, and service communications	Controller for account administration; processor for customer-defined user administration where applicable	Contract where the individual is a party; otherwise legitimate interests in providing and administering the customer relationship and Services.
Negotiate and administer contracts, subscriptions, invoicing, accounting, and tax records	Controller	Contract; legal obligation; and legitimate interests in business administration, debt recovery, and record keeping.

Activity and purpose	TraCerLab role	GDPR / UK GDPR basis when TraCerLab is controller
Process customer-controlled content to provide configured Services	Processor	The customer determines the lawful basis. TraCerLab acts on documented instructions and does not assign an independent Article 6 basis merely because it supplies the technology.
Secure the Services, authenticate access, maintain auditability, investigate incidents, and prevent abuse, fraud, or unauthorised access	Controller for independently determined security; processor where done solely on customer instructions	Legitimate interests in security, integrity, safety, fraud prevention, and defence of rights; legal obligation where a specific duty applies.
Conduct proportionate identity, counterparty, restricted-party, or eligibility checks for TraCerLab's own access, safety, or compliance decisions	Controller	Legal obligation where a specific law binds TraCerLab; otherwise legitimate interests in lawful operations, service integrity, fraud prevention, and protection of customers and third parties. Any special-category or offence data requires an additional condition.
Enable customer-configured identity, document, due-diligence, compliance, safety, or transaction workflows	Processor, unless a specific independent purpose is separately disclosed	The customer determines the lawful basis and any Article 9 or 10 condition.
Support multi-party collaboration or transaction features and protect their integrity	Processor for customer-controlled records; independent or joint controller only for specifically identified safety, fraud, or shared-purpose processing	Legitimate interests, legal obligation, or another disclosed basis. Any joint-control activity is covered by a specific Article 26 arrangement.
Provide extraction, search, scoring, anomaly detection, classification, analytics, prediction, assistants, or other automated functionality requested through the Services	Processor for customer-controlled inputs and purposes; controller for any separately disclosed TraCerLab purpose	Customer's basis when processor. For ordinary advisory processing as controller: contract, legitimate interests, or consent, depending on the feature and impact. A solely automated decision with legal or similarly significant effects is made only under a specific exception permitted by applicable law and with the safeguards in Section 9.
Measure reliability and performance; troubleshoot; develop, test, and improve accessibility, usability, security, and functionality	Controller for limited operational telemetry; processor for customer content used only on instruction	Legitimate interests in improving and protecting the Services, balanced against individual rights; consent for non-essential device storage or access where required. Customer content is used for TraCerLab's own general model training only under Section 9.5.
Send requested, administrative, security, service, or legal communications	Controller, or processor for customer-directed messages	Contract, legal obligation, and legitimate interests in administering and securing the relationship.
Send business-to-business news, event, or marketing communications	Controller	Consent where required; otherwise legitimate interests in proportionate business marketing, subject to electronic-marketing law and an unconditional right to opt out.
Store or access information on a device through cookies or similar technology	Controller	Consent where required; strictly necessary or another statutory exception where applicable; resulting Personal Data is processed under the corresponding Article 6 basis.
Receive and resolve privacy requests, complaints, ethics reports, disputes, legal claims, audits, and regulatory or lawful-access requests	Controller	Legal obligation; legitimate interests in compliance, investigation, protection of rights, and establishment, exercise, or defence of claims.
Protect life, physical safety, or critical interests in a genuine emergency	Controller or processor depending on configuration	Vital interests where strictly necessary; otherwise contract, legitimate interests, legal obligation, or customer instructions.
Recruit personnel and manage supplier or adviser relationships	Controller	Steps before a contract, contract, legal obligation, and legitimate interests in recruitment, due diligence, and relationship management; additional conditions for sensitive data.

Activity and purpose	TraCerLab role	GDPR / UK GDPR basis when TraCerLab is controller
Reorganise, finance, audit, acquire, or transfer all or part of the business	Controller	Legitimate interests in responsible corporate operations and transactions; legal obligation where applicable, subject to confidentiality and data minimisation.

6.1 Legitimate interests

Where TraCerLab relies on legitimate interests, the relevant interests may include operating and improving a business technology service; providing and administering the Services; information and physical security; fraud and abuse prevention; service integrity; auditability; customer and third-party protection; limited professional marketing; business continuity; and establishing, exercising, or defending legal rights. TraCerLab considers necessity, reasonable expectations, data sensitivity, potential impact, and available safeguards. You may object as described in Section 16.

6.2 Consent

Where processing is based on consent, consent is specific to the stated purpose, can be refused where the processing is optional, and can be withdrawn as easily as it was given. Withdrawal does not affect processing already lawfully carried out. If data is objectively necessary to provide a requested contractual Service, TraCerLab does not describe consent as the basis merely because the user clicked an acceptance box.

6.3 New or compatible purposes

TraCerLab will not use controller Personal Data for an incompatible new purpose without first completing the assessment and taking the steps required by law, which may include an updated notice and new consent. When acting as processor, TraCerLab requires new or amended documented instructions from the customer.

7. When providing data is required

Certain identity, business contact, account, authentication, contract, billing, or security fields are necessary to create an account, enter or administer a contract, provide a requested Service, meet a legal requirement, or keep the Services secure. If required data is not provided, TraCerLab may be unable to create or maintain the account, provide the relevant feature, complete a requested transaction, or meet the legal requirement.

Other fields and optional features are voluntary and are identified as such where practicable. Identity documents, precise location, photographs, safety data, or other sensitive information are requested only when the applicable feature, customer instruction, or law requires them. A customer or public authority may impose its own requirements and must explain those requirements in its notice.

8. Cookies and similar technologies

TraCerLab may use cookies, local storage, pixels, software development kits, or similar storage and access technologies on its websites and Services. Where a website or Service uses such technology, a cookie preference control or collection-point notice identifies the technologies in current use, their provider, purpose, category, third-party access, and duration. That live notice is the authoritative point-in-time inventory.

Category	Purpose	Choice and retention approach
Strictly necessary	Authentication, session continuity, security, network delivery, fraud prevention, and recording privacy choices	Used without consent only where a legal exception applies. Retained only for the session or the period necessary for the stated function and proof of choice. Disabling them may prevent the Service from working.
Functional or preference	Language, region, accessibility, interface, and optional convenience settings	Used with consent where required, unless a specific statutory exception applies. Retained only while the preference remains relevant.

Category	Purpose	Choice and retention approach
Analytics or performance	Audience measurement, error diagnosis, performance, reliability, and feature usage	Disabled until valid consent where consent is required, unless a narrow statutory exception applies. Individual-level data is kept only as long as needed for the stated measurement.
Embedded or integration technology	User-requested maps, media, communications, support, identity, or payment functionality	The relevant provider and purpose are disclosed in the preference control or at the point of use. Consent is obtained unless necessary for a requested function or another exception applies.
Advertising	TraCerLab does not use these technologies to sell Personal Data or for third-party targeted advertising.	Not applicable under current practices.

Where consent is required, non-exempt technology is blocked until a user makes an affirmative choice. Rejecting non-essential technology must be as accessible as accepting it, and consent can be changed through the privacy or cookie control made available on the relevant website or Service. Browser controls can provide additional control but are not the sole withdrawal method offered by TraCerLab.

9. AI, profiling, and automated decision-making

9.1 Uses, inputs, logic, and outputs

Depending on the configured Service, TraCerLab may provide rules-based, statistical, machine-learning, or other automated features for:

- document extraction, search, summarisation, translation, and assistance;
- data-quality, completeness, consistency, or anomaly checks;
- identity, entity, registry, or restricted-party matching;
- security, fraud, abuse, and workflow monitoring;
- similarity, confidence, risk, prioritisation, classification, or prediction signals; and
- operational, geospatial, scientific, or aggregate analytics.

Inputs may include the data categories described in Section 4. The principal factors are the submitted or authorised source data, relevant reference data, configured rules or criteria, and recorded workflow events. Outputs may include extracted fields, matches, alerts, flags, classifications, scores, confidence ranges, recommendations, or proposed actions. Data quality, context, configuration, and system limitations can produce false positives, false negatives, or other errors.

9.2 Consequences and human oversight

Unless expressly identified otherwise in a feature-specific notice, automated outputs are advisory and intended to support qualified human review. They must not be treated as legal certification or used as the sole basis for an enforcement, employment, credit, insurance, healthcare, legal, or similarly significant decision unless the use complies with all applicable legal conditions and safeguards.

An automated output may affect how a record, request, transaction, or account is prioritised, reviewed, or made available. Where TraCerLab is controller and a decision produces legal or similarly significant effects, TraCerLab will not base that decision solely on automated processing unless applicable law permits it. It will provide the notice, lawful basis, meaningful information, and safeguards required in the relevant jurisdiction, including a way to make representations, contest the result, and obtain review by a person who understands the output and has authority to change the decision.

Where a customer configures or makes a decision using an automated feature, the customer is ordinarily responsible for assessing whether its use constitutes profiling or significant automated decision-making and for providing the required notice, lawful basis, impact assessment, human review, and appeal. TraCerLab assists as required by the DPA.

9.3 Information and challenges

Where required, an affected person may request information about the categories of input that affected an output, the type and use of the output, the main reasons or factors, and the available review process. Trade secrets and security-sensitive information may be protected, but not used to withhold information that law requires.

9.4 AI interaction transparency

Where required by law and not already obvious from context, the interface identifies when a person is interacting directly with an AI system or receiving AI-generated content. Materially deceptive synthetic content is not knowingly presented as authentic human-generated content.

9.5 Training and improvement

TraCerLab may use operational telemetry and feedback that it controls, test data that contains no Personal Data, and irreversibly anonymised or aggregate information to evaluate and improve the Services and analytical systems. TraCerLab does not use customer-controlled Personal Data to train a general-purpose model for its own purposes. Where a third-party model provider processes customer-controlled Personal Data on TraCerLab's behalf, TraCerLab requires that provider not to use the data to train a general-purpose model for either party's own purposes. If TraCerLab proposes a materially different use in the future, it will not begin that use unless it has first amended the applicable contractual terms, completed the required assessment, established a valid lawful basis and any additional sensitive-data condition, and provided any required notice and choice.

Information that is merely pseudonymised or de-identified but still reasonably linkable is treated as Personal Data. TraCerLab does not attempt to re-identify information represented as anonymous.

10. Communications and marketing

TraCerLab may send account, transaction, security, support, service, legal, and other non-marketing communications needed to administer a relationship or requested Service. A user may not be able to opt out of a strictly necessary communication while the relevant account or relationship remains active.

Marketing communications are sent only as permitted by applicable direct-marketing and electronic-communications law. Every electronic marketing message provides an unsubscribe method, and an objection to direct marketing is honoured without requiring reasons. TraCerLab may retain a minimal suppression record so that the opt-out remains effective.

When a customer uses the Services to send messages, TraCerLab ordinarily acts as processor. The customer is responsible for the recipient list, lawful basis, notice, content, and required opt-out or consent. A recipient may contact the customer or TraCerLab if the customer's identity is unclear.

11. Who receives Personal Data

TraCerLab discloses only the data reasonably necessary for the relevant purpose. Recipients may include:

Recipient	Circumstances and safeguards
The relevant customer and authorised users	Account administrators, authorised personnel, and other users receive data according to configured permissions, workflow rules, and the customer's instructions.
Authorised counterparties or participants	Data may be shared through a customer-configured collaboration, transaction, verification, export, or public-sharing function. The interface or customer determines the audience.
Processors and subprocessors	Technical and operational providers supporting service delivery, identity and access, security, communications, support, analytics, mapping, document or automated processing, and payment or billing. Contracts impose confidentiality, security, purpose, and data-protection duties appropriate to the role.
Customer-authorised integrations and independent providers	A user or customer may direct data to or from an external system. Some providers may act as independent controllers for part of the processing and provide their own notice.
Professional advisers and assurance providers	Lawyers, accountants, auditors, insurers, banks, and security or compliance advisers, subject to professional or contractual confidentiality.

Recipient	Circumstances and safeguards
Authorities and legal recipients	Courts, regulators, law enforcement, tax or public authorities, and parties to legal proceedings, only where disclosure is required or permitted and Section 15 is followed.
Corporate transaction recipients	A prospective or actual investor, financier, buyer, seller, successor, or restructuring party under confidentiality and due-diligence controls.
Emergency recipients	A customer-designated safety contact or competent emergency recipient where strictly necessary to protect life or safety and legally permitted.
The public	Only where the customer or user intentionally uses a public page or sharing function, or where law requires publication. Users must not publish unnecessary Personal Data.

TraCERLab maintains a separate, current Subprocessor and Transfer Register identifying each provider, its function, relevant processing location or locations, and the applicable transfer mechanism where required. A customer may request the register information applicable to its processing under the DPA, and an affected person may request the identity of actual recipients of their Personal Data where applicable law grants that right. Information may be redacted or disclosed through a confidential process only to the extent permitted by law and necessary to protect the rights of others, confidential information, or security.

11.1 No sale or third-party targeted advertising

TraCERLab does not sell Personal Data or use Personal Data for third-party targeted advertising.

If these practices materially change, TraCERLab will update the relevant notice before the new practice begins and provide any opt-out, restriction, or consent mechanism required by applicable law.

11.2 Public sharing

Where a customer or user intentionally uses a public-sharing feature, the information may become visible to others and may be copied outside TraCERLab's control. TraCERLab provides a contextual warning where the consequence is not already obvious. Users must not publish Personal Data unless authorised and necessary. Non-public records remain subject to the ordinary retention and rights rules.

12. International processing and transfers

Personal Data may be accessed, supported, or processed outside the country where it was collected. Before a restricted international transfer occurs, TraCERLab identifies the destination country or international organisation, the relevant roles and data categories, and the lawful transfer mechanism. The applicable collection-point notice identifies material destination countries where required, and an affected person may request information about the destination and relevant safeguards through privacy@tracerlabgroup.com.

For a restricted transfer from the European Economic Area, TraCERLab relies on an applicable adequacy decision or another lawful mechanism for the actual roles, including the European Commission's Standard Contractual Clauses, together with a transfer assessment and supplementary measures where required.

For a restricted transfer from the United Kingdom, TraCERLab uses an applicable UK adequacy regulation, the UK International Data Transfer Agreement, or the UK International Data Transfer Addendum to the EU Standard Contractual Clauses, and applies the required data-protection test or transfer assessment.

Where legally available, TraCERLab may rely on an approved certification framework only if the recipient is actively certified and the transfer is within scope. Statutory derogations are used only where appropriate for the specific transfer, not as a routine substitute for safeguards.

TraCERLab applies contractual onward-transfer restrictions and proportionate technical and organisational safeguards. To request more information or a copy of the relevant safeguard, subject to redaction of confidential and security-sensitive terms, email privacy@tracerlabgroup.com.

13. Security and privacy governance

TraCERLab uses technical and organisational measures designed to provide security appropriate to the nature, scope, context, and risk of processing. These include proportionate governance, access, confidentiality, data-protection,

oversight, incident-management, continuity, supplier, and personnel measures. For each material processing activity, TraCerLab's internal records identify the applicable controller or processor role, purpose, lawful basis, data categories, recipients, retention, international transfers, and any required data protection impact assessment.

Additional security information may be provided through an authorised confidential due-diligence process where appropriate.

No internet transmission or storage system can be guaranteed completely secure. This statement does not reduce any duty imposed by law or contract. Users must protect credentials and devices, follow customer security instructions, and promptly report suspected compromise to security@tracerlabgroup.com. Do not send credentials or unnecessary identity documents by ordinary email.

13.1 Personal Data breaches

If a suspected Personal Data breach occurs, TraCerLab will identify, contain, investigate, document, and remedy it and take reasonable steps to reduce recurrence.

- When TraCerLab is controller, it notifies the competent supervisory authority within 72 hours after becoming aware where GDPR or UK GDPR requires notification, and notifies affected individuals without undue delay where the breach is likely to result in the legally specified high risk.
- When TraCerLab is processor, it notifies the relevant customer without undue delay and provides the information and assistance required by the DPA. The customer determines its own regulatory and individual notifications unless applicable law assigns responsibility otherwise.
- In other jurisdictions, TraCerLab follows the applicable content and timing requirements.

Notification may be delayed or limited only where law permits, including to preserve an investigation or avoid increasing security risk.

14. Retention, deletion, and legal holds

TraCerLab retains Personal Data only for the period reasonably necessary for the disclosed purpose, documented customer instructions, security and continuity, applicable law, and the establishment, exercise, or defence of legal claims. The following criteria apply. Where TraCerLab has approved a fixed retention period for a category of Personal Data, that period is recorded in its retention schedule and stated in the relevant collection-point or feature-specific notice where appropriate:

Category	Retention criterion
Website enquiries, prospects, events, and ordinary business contacts	While the enquiry or relationship is active and thereafter only for a documented follow-up, limitation, dispute, or legal-compliance period.
Account, authentication, and professional-user administration	For the account or contractual relationship and the period needed afterwards for security, audit, contractual, limitation, or legal obligations.
Customer-controlled content	Under the customer's documented instructions and agreement, including any agreed return or export period, subject to regulated or evidentiary records that the customer lawfully instructs TraCerLab to retain.
Identity, due-diligence, compliance, transaction, accounting, and evidentiary records	For the period required by the applicable customer instruction, sector rule, accounting or tax law, limitation period, or documented evidentiary need. Requirements differ by jurisdiction and record type.
Audit, access, security, and integrity data	For the period necessary to detect and investigate misuse, reconstruct relevant events, demonstrate compliance, resolve an incident, or defend a claim, then deleted or anonymised.
AI and automated-processing accountability data	For the period needed to provide the feature, monitor material performance or risk, explain or contest a result, meet an accountability duty, or follow the customer's lawful instruction. Unnecessary prompt content is minimised.
Communications and support records	Until the communication or case is resolved, and longer only where incorporated into a contract, transaction, complaint, safety record, investigation, or legal matter.

Category	Retention criterion
Recruitment and supplier records	For the selection or relationship process and the period required for legal, equality, limitation, due-diligence, or claim purposes.
Privacy choices, requests, complaints, and investigations	For as long as necessary to implement and prove the choice, resolve the matter, meet recordkeeping duties, and defend rights.
Cookies and similar identifiers	As stated in the live collection-point or cookie notice for the relevant technology.
Residual copies	Handled under documented retention and deletion procedures, subject to applicable law and legal holds.

TraCerLab may suspend deletion for a narrowly scoped legal hold, litigation, audit, regulatory request, fraud or security investigation, or preservation duty. Access is restricted and ordinary deletion resumes when the hold ends. Data is deleted, anonymised, or returned in accordance with documented procedures and the applicable agreement. Irreversibly anonymised information may be retained without a Personal Data retention limit.

15. Government, regulatory, emergency, and lawful-access requests

When TraCerLab receives a request for Personal Data from an authority, it will, to the extent legally permitted and appropriate:

- verify the requester's identity, competence, jurisdiction, legal basis, form, and scope;
- distinguish a binding demand from a voluntary request;
- redirect the authority to the customer or primary controller where appropriate;
- seek clarification, narrow an overbroad request, or challenge it where there are reasonable legal grounds;
- disclose only the data legally required and use a secure method;
- preserve confidentiality and a record of the decision; and
- notify the affected customer or individual before disclosure unless prohibited by law or where notice would create a legally recognised risk.

TraCerLab may disclose the minimum necessary information in a genuine emergency involving a credible threat to life or physical safety where applicable law permits. Emergency disclosure is documented and reviewed.

16. Your privacy rights and how to exercise them

Depending on the law and TraCerLab's role, you may have the right to:

- receive information about processing and obtain access to your Personal Data;
- obtain the identity of actual recipients where applicable law grants that right;
- correct inaccurate or complete incomplete Personal Data;
- request deletion;
- restrict or object to processing, including an unconditional objection to direct marketing;
- receive Personal Data you provided in a structured, commonly used, machine-readable format and transmit it to another controller where portability applies;
- withdraw consent at any time;
- obtain information, make representations, contest a result, and request human intervention for a qualifying significant automated decision;
- complain to a competent supervisory authority or regulator.

Rights are subject to conditions and exceptions. For example, TraCerLab may retain data needed to provide a requested Service, protect security, comply with law, preserve freedom of expression, establish or defend claims, or meet a documented customer instruction where the customer remains controller.

16.1 Submitting a request

Email privacy@tracerlabgroup.com with the subject "Privacy Rights Request" and describe:

- your name and preferred contact method;
- the right you wish to exercise;
- the relevant account, customer organisation, Service, or interaction; and
- enough context to locate the data without sending unnecessary sensitive information.

TraCerLab may request proportionate information to verify identity, authority, jurisdiction, and scope. Verification information is used only to handle the request and related legal duties. Never send a password, authentication secret, or full identity document unless TraCerLab specifically requests it through a secure method.

An authorised agent may submit a request where law permits. TraCerLab may require evidence of authority and, where permitted, direct confirmation from the individual. A person does not need to create a new account to make a request, although an existing authenticated account may be used for verification.

16.2 Requests concerning customer-controlled data

If TraCerLab processes the relevant data only on behalf of a customer, TraCerLab will ordinarily identify or refer the request to that customer and will assist it under the DPA. TraCerLab will not independently delete or alter customer-controlled evidence or records contrary to a lawful controller instruction. If you cannot identify the customer, provide the context and TraCerLab will take reasonable steps to route the request without disclosing another person's confidential information.

16.3 Timing and fees

For EU GDPR requests, TraCerLab responds without undue delay and ordinarily within one month. Where complexity or volume permits an extension of up to two further months, TraCerLab gives notice and reasons within the initial one-month period.

For UK requests, the statutory period begins and is calculated as applicable UK law provides. A permitted request for clarification of a subject access request pauses the running period and the remaining time resumes when clarification is received; it does not restart a full response period. TraCerLab may extend by up to two further months where law permits and will give timely reasons.

Requests are ordinarily free. TraCerLab may charge a reasonable fee or refuse to act only where applicable law permits, such as for a manifestly unfounded or excessive request, and will explain the decision and available complaint or appeal route.

17. Regional notices

17.1 European Economic Area and Belgium

TraCerLab SC is established in Belgium and is the controller for the activities identified as controller processing in this Policy. Individuals in the European Economic Area have the rights in Articles 12-22 GDPR subject to their legal conditions. They may lodge a complaint with the authority in the Member State of habitual residence, place of work, or alleged infringement, and may seek a judicial remedy. A list of supervisory authorities is available from the European Data Protection Board at https://www.edpb.europa.eu/about-edpb/about-edpb/members_en.

TraCerLab's principal authority for processing connected with its Belgian establishment is:

Belgian Data Protection Authority / Autorité de protection des données / Gegevensbeschermingsautoriteit Rue de la Presse / Drukpersstraat 35, 1000 Brussels, Belgium Telephone: +32 (0)2 274 48 00 Email: contact@apd-gba.be
Website: <https://www.dataprotectionauthority.be/>

Contacting TraCerLab first is welcome but is not a condition of complaining to an authority.

17.2 United Kingdom

Where UK data-protection law applies, references in this Policy include the UK GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations, and amendments made by the Data (Use and Access) Act 2025. UK residents have the applicable rights described in Section 16.

For a significant decision based solely on automated processing, TraCerLab applies the required safeguards, including information about the decision, a way to make representations, human intervention, and a way to contest the decision. Special-category data receives the additional restrictions required by UK law.

A person may make a data-protection complaint through privacy@tracerlabgroup.com. Where the UK statutory complaints procedure applies, TraCerLab acknowledges the complaint within 30 days, investigates it, keeps the complainant appropriately informed, and communicates the outcome without undue delay. A person may also complain to the Information Commissioner's Office at <https://ico.org.uk/make-a-complaint/>.

17.3 Democratic Republic of the Congo

Where processing is governed by the Democratic Republic of the Congo's Digital Code, this subsection supplements this Policy and prevails to the extent it provides stricter protection.

At or before collection, the relevant controller provides a clear and accessible notice identifying the controller and, where applicable, its mandated representative and data-protection officer; the purposes and categories of Personal Data; recipients; whether providing the data is compulsory or optional and the consequences of not providing it; the applicable retention period; any proposed transfer outside the Democratic Republic of the Congo; and, where relevant, meaningful information about automated decision-making or profiling, its significance, and its expected consequences. Where Personal Data is obtained from another source, the information is provided within the period and by the first event required by applicable law, unless a documented legal exception applies.

Subject to applicable conditions and exceptions, individuals may request information and access, correction or updating, restriction or blocking, objection, deletion or erasure, and portability where applicable; withdraw consent; complain to the competent authority; and give legally recognised instructions concerning the retention, deletion, communication, or transmission of their Personal Data after death. Requests may be submitted through privacy@tracerlabgroup.com.

A processing activity or international transfer governed by the Democratic Republic of the Congo's law is undertaken only after any required declaration, authorisation, local-handling condition, and other statutory safeguard has been satisfied. Section 12 does not itself authorise a transfer prohibited by that law.

18. Children and minors

The Services are not directed to children, and a person under 18 or the age of legal majority in the relevant jurisdiction may not create an account. TraCerLab does not knowingly collect a child's Personal Data as controller for consumer marketing, behavioural advertising, or account registration.

Customer-controlled records may nevertheless concern a minor in an authorised safeguarding, labour-risk, community, research, safety, regulatory, or evidentiary context. In that situation, the customer is ordinarily the controller and must establish a lawful basis, use an age-appropriate and local-language notice where required, obtain parental or other authorisation where required, minimise the data, and restrict access. TraCerLab applies the customer's lawful instructions and DPA safeguards.

If TraCerLab learns that it has collected a child's Personal Data as controller contrary to this section, it will restrict and delete it as required. A parent, guardian, or affected person may contact privacy@tracerlabgroup.com.

19. Data accuracy, third-party sources, and user responsibilities

TraCerLab takes reasonable steps to keep controller Personal Data accurate for its stated purpose. Information from a customer, public registry, regulatory list, map, integration, or other third party may be incomplete, delayed, or inaccurate. An individual may challenge a TraCerLab-controlled record under Section 16. Correcting an authoritative external source may also require a request to that source or the relevant customer.

Customers and users must:

- submit Personal Data only where authorised and necessary for an approved purpose;
- provide required privacy notices and obtain any required permission;
- keep account and submitted information reasonably accurate;
- avoid placing Personal Data in public or free-text fields not intended for it;

- use appropriate access permissions and respect confidentiality; and
- promptly correct or report material inaccuracies and unauthorised disclosure.

These responsibilities do not reduce TraCerLab's own obligations or an individual's statutory rights.

20. Changes to this Policy

TraCerLab reviews this Policy periodically and before materially new controller processing. The current version and Last Updated date are published with the Services.

For a material change, such as a new sensitive-data purpose, sale or use for third-party targeted advertising, qualifying significant automated decision, materially different recipient category, or materially different international transfer, TraCerLab provides prominent advance notice through the relevant website, Service, or registered contact within the period required by applicable law. It obtains new consent where law requires consent. A non-material clarification, legal update, formatting change, or correction may take effect on publication.

Continued use does not convert this Policy into consent. Previous versions are retained where required by law or needed to demonstrate the notice that applied to relevant processing.

21. Contact, complaints, and accessibility

Purpose	Contact
Privacy information, rights request, or complaint	privacy@tracerlabgroup.com
Suspected security incident	security@tracerlabgroup.com
General legal enquiry	legal@tracerlabgroup.com
Registered office	TraCerLab SC, Avenue Marcel Gourdin 60, 5001 Namur, Belgium; VAT BE0758359658 www.tracerlabgroup.com

Address privacy correspondence to Privacy Contact. Where applicable law requires a data-protection officer or local representative, the relevant notice identifies that person or organisation and provides the required contact details. TraCerLab may move a sensitive exchange to a secure channel.

This Policy is intended to be readable, printable, and accessible. To request it in an alternative format or another language used for a relevant deployment, email privacy@tracerlabgroup.com. A more specific local-language notice may be delivered at the collection point, including through an offline interface where connectivity is limited.

Privacy disputes under a customer agreement remain subject to that agreement only to the extent permitted by mandatory law. Nothing in an agreement or this Policy restricts a non-waivable right to contact a regulator, lodge a complaint, or seek a judicial remedy.

End of , Version 3.0.