

ALIAS Intel Privacy Policy

Effective date: August 4, 2026

This Privacy Policy explains how ALIAS Intel, Québec enterprise number NEQ 2282422304, collects, uses, communicates, retains and protects personal information through its website, aerospace and defence intelligence platform, reports, notifications and related services collectively referred to as the “Service.”

It applies to website visitors, prospective customers, customers, authorized users, report recipients and others who communicate with or use ALIAS Intel.

ALIAS Intel is responsible for the personal information under its control.

1. Personal information we collect

The information collected depends on how an individual interacts with ALIAS Intel.

Account and contact information

This may include:

- name;
- business email address and telephone number;
- job title, employer and country or region;
- account credentials;
- account and communication preferences; and
- information provided through sales, demonstrations, onboarding, support requests, surveys, meetings or other communications.

Customer profiles and Service configuration

Customers may provide information used to configure their intelligence feeds, including:

- company, product and capability information;
- customers, markets, interests and business priorities;
- names and email addresses of authorized users and report recipients;
- saved preferences; and
- feedback regarding matches, reports and Service performance.

Much of this information concerns organizations. Where it identifies or can reasonably be associated with an individual, ALIAS Intel treats it as personal information.

Subscription and transaction information

This may include:

- subscription plan and billing contact;
- billing country and tax-registration information;
- transaction dates and amounts;
- payment status; and
- records relating to trials, renewals, cancellations and refunds.

Payments are processed by third-party payment processors such as Stripe. ALIAS Intel does not normally receive or retain complete payment-card numbers.

Usage and technical information

When someone visits the website or uses the Service, ALIAS Intel may automatically collect:

- Internet Protocol address;
- browser, device and operating-system information;
- login and account activity;
- features, reports and intelligence items accessed;
- dates and times of access;
- referring website;
- approximate location derived from an Internet Protocol address;
- diagnostic and performance information; and
- security and audit logs.

Public-source business information

The Service monitors public, commercial and government sources that may contain names, professional titles, organizational affiliations, authorship information and publicly available business contact information.

ALIAS Intel uses this information where relevant to providing aerospace and defence business intelligence.

2. How information is collected

ALIAS Intel may collect personal information:

- directly from the individual;
- from the individual's employer, organization or account administrator;
- automatically through the website or Service;
- through cookies and similar technologies;
- from payment, authentication and other service providers; and
- from public, government and commercial information sources.

Customers are responsible for ensuring that they are authorized to provide the personal information of users, recipients, employees and other contacts to ALIAS Intel.

3. How information is used

ALIAS Intel may use personal information to:

- create, authenticate and administer accounts;
- provide, configure and personalize the Service;
- match information against Customer profiles and priorities;
- generate intelligence feeds, reports, summaries, classifications and relevance scores;
- distribute reports and notifications to authorized recipients;
- process subscriptions and payments;
- provide demonstrations, onboarding and support;
- communicate about accounts, subscriptions and Service changes;
- respond to inquiries and requests;
- understand and improve use, matching accuracy and Service performance;
- diagnose technical problems;
- protect accounts, systems and information;
- prevent fraud, misuse and unauthorized access;
- maintain business, tax and transaction records;
- enforce agreements and policies;
- comply with legal obligations; and
- create aggregated or de-identified statistics that do not identify an individual or disclose Customer confidential information.

ALIAS Intel limits collection and use to information reasonably necessary for these purposes.

4. Artificial intelligence and automated processing

The Service uses automated systems, matching algorithms and artificial intelligence to monitor information, identify potential relevance, classify content, generate summaries and personalize Customer intelligence feeds.

Customer profiles, source content and related information may be processed by technology and artificial-intelligence service providers acting on behalf of ALIAS Intel.

Authorized personnel may review Customer profiles, source content, matches, feedback and generated outputs to configure the Service, provide support and improve performance.

ALIAS Intel does not use the Service to make decisions about individuals that produce legal or similarly significant effects, such as decisions concerning employment, credit, insurance or eligibility.

ALIAS Intel does not sell Customer Data or intentionally make it available to train a public or shared artificial-intelligence model for unrelated third-party purposes.

Customers must not submit classified information, Controlled Unclassified Information, export-controlled technical data, information controlled under the International Traffic in Arms Regulations, controlled goods information or other restricted information through the Service.

5. Cookies and similar technologies

ALIAS Intel may use cookies, browser storage and similar technologies to:

- authenticate users and maintain login sessions;
- remember preferences;
- protect accounts and prevent misuse;
- support website and Service functionality;
- diagnose performance problems; and
- understand general website and Service usage.

Technologies necessary for authentication, security and core functionality may operate automatically.

Where optional analytics or similar technologies are used, available consent or preference controls will be provided where required by law.

Browser settings may also be used to block or delete cookies, although blocking essential cookies may prevent parts of the Service from functioning.

ALIAS Intel does not use personal information for third-party behavioural advertising.

6. When information is communicated

ALIAS Intel may communicate personal information where reasonably necessary to the following recipients.

Service providers

Providers may support:

- cloud hosting, databases and infrastructure;
- authentication and security;
- payment processing;
- email delivery;
- artificial-intelligence processing;
- analytics and diagnostics;
- customer support; and
- legal, accounting and other professional services.

These providers may process personal information only for the services they provide to ALIAS Intel and are expected to protect it appropriately.

Customer organizations

Account, usage and Service information may be available to the Customer organization that purchased or administers the subscription, including its authorized account administrators.

Individuals using an account provided by an organization should understand that the organization may administer the account and control its Customer Data.

Legal and business purposes

ALIAS Intel may communicate information where reasonably necessary to:

- comply with law, a court order or lawful government request;
- protect the rights, safety or property of ALIAS Intel, its customers or others;
- investigate fraud, unlawful conduct or a security incident;
- enforce an agreement;
- obtain professional advice; or
- complete a proposed or completed financing, reorganization, merger, acquisition, asset sale or transfer of the Service.

Information may also be communicated for another purpose with consent or where otherwise permitted by law.

ALIAS Intel does not sell or rent personal information.

7. Processing outside Québec and Canada

ALIAS Intel operates from Québec but uses service providers that may process or retain personal information elsewhere in Canada, the United States or other jurisdictions.

Information may therefore be subject to the laws of the jurisdiction where it is processed and may be accessible to courts, law-enforcement agencies or government authorities in accordance with those laws.

Before entrusting personal information to a provider outside Québec, ALIAS Intel assesses the arrangement and applies contractual, organizational and technical protections appropriate to the information and applicable legal requirements.

8. Retention and destruction

ALIAS Intel retains personal information only as long as reasonably necessary to:

- provide the Service and maintain the Customer relationship;
- complete transactions and provide support;
- protect the security and integrity of the Service;
- resolve disputes and enforce agreements; and
- meet legal, tax, accounting and regulatory obligations.

Retention periods vary according to the information and its purpose.

Account and Customer configuration information is generally retained while the account is active and for a reasonable period afterward. Transaction and business records may be retained longer where legally required. Technical logs, security records and backups are retained according to operational and security schedules.

When information is no longer required, ALIAS Intel will destroy it or anonymize it for a serious and legitimate purpose, subject to legal retention requirements and reasonable backup cycles.

9. Safeguards and security incidents

ALIAS Intel uses reasonable administrative, technical and organizational safeguards appropriate to the sensitivity, amount, use and format of the personal information under its control.

These safeguards may include:

- access restrictions and authentication controls;
- encryption where appropriate;
- secure hosting and communications;
- monitoring and backups;
- confidentiality obligations;
- service-provider controls; and
- incident-response procedures.

Access is limited to authorized individuals and providers who require the information to perform their duties.

No internet-based system can be guaranteed to be completely secure. Users should protect their credentials and promptly report suspected unauthorized access.

Where a confidentiality or security incident creates a legally reportable risk, ALIAS Intel will take appropriate steps and provide required notifications.

10. Individual rights

Depending on applicable law and the circumstances, an individual may have the right to:

- confirm whether ALIAS Intel holds personal information about them;
- access that information;
- request correction of inaccurate, incomplete or ambiguous information;
- withdraw consent to certain uses or communications;
- request deletion or anonymization where applicable;
- request cessation of dissemination or de-indexing where applicable;
- receive eligible computerized information in a structured, commonly used format;
- object to or restrict certain processing where applicable;
- unsubscribe from marketing communications; and
- submit a privacy complaint.

Requests must be submitted in writing to the ALIAS Intel Privacy Officer. ALIAS Intel may request information necessary to verify identity and authority before responding.

ALIAS Intel will respond within the period required by applicable law. Rights may be limited where information must be retained to comply with law, complete a transaction, protect security, preserve legal rights or fulfil a contractual obligation.

Withdrawal of consent does not affect processing already lawfully completed and may prevent ALIAS Intel from providing some features.

Where information originated from a third-party publication or public source, ALIAS Intel may correct or remove its own record where appropriate but does not control the original source.

11. Communications

ALIAS Intel may send communications necessary to provide the Service, including:

- account and security notices;
- subscription and payment communications;
- intelligence feeds and reports;
- requested notifications;
- support communications; and
- notices of material Service or policy changes.

These communications may continue while an account remains active.

ALIAS Intel may also send information about its products or services where permitted by law. Marketing communications will include an available method to unsubscribe.

Unsubscribing from marketing does not prevent necessary account, transaction, security or Service communications.

12. Children and third-party websites

The Service is intended for professional and business use and is not directed to individuals under 18 years of age.

ALIAS Intel does not knowingly collect personal information directly from children. Anyone who believes a child has provided information to ALIAS Intel should contact the Privacy Officer.

The Service may link to or display information from third-party websites, publications and government systems. This Privacy Policy does not govern those third parties, and individuals should review their applicable privacy policies.

13. Changes to this Privacy Policy

ALIAS Intel may update this Privacy Policy to reflect changes to the Service, business practices, technology or legal requirements.

The effective date identifies when it was last updated. Material changes will be communicated through the website, Service, email or another reasonable method where required by law.

14. Privacy Officer and contact

The person responsible for the protection of personal information at ALIAS Intel is the:

Privacy Officer

ALIAS Intel

Québec enterprise number: NEQ 2282422304

info@alias-intel.com

Questions, access or correction requests, consent withdrawals and privacy complaints may be submitted to info@alias-intel.com.

ALIAS Intel will review complaints and respond within a reasonable period. Individuals may also have the right to contact the privacy or data-protection regulator applicable to their jurisdiction.