

General Terms of Sale and Use of the SAMRoute Service

Oriskami SAS

19 mai 2025

1	PREAMBLE	1
2	PURPOSE	2
3	ACCESS RIGHTS	2
4	CONTRACT LIFECYCLE	3
5	PRICING	5
6	PAYMENT	6
7	CLIENT'S COMMITMENTS	6
8	PROVIDER'S COMMITMENTS	7
9	AVAILABILITY	8
10	DATA PROTECTION	9
11	INTELLECTUAL PROPERTY	10
12	CLIENT RIGHTS UPON EXIT	11
13	APPLICABLE LAW AND JURISDICTION	11
<hr/>		
A	SERVICE LEVEL AGREEMENT (SLA)	13
B	CONFIDENTIALITY	14
C	DEFINITIONS	16
D	CONTENTS	18

1 PREAMBLE

This contract governs access to the SAMRoute software, published by Oriskami SAS, for strictly professional use. It is suited to varying levels of commitment, from exploratory projects to multi-year collaborations. These Terms apply to two types of Clients, depending on subscription and billing methods :

- ENTERPRISE Clients have a direct relationship, formalized through a quote or purchase order. No tacit renewal applies. They may terminate at any time with a partial refund of the unused period.
- Other Clients (non-ENTERPRISE) follow a simplified process, with monthly billing via automatic debit (Stripe). The contract is open-ended, tacitly renewed each month, and can be terminated at any time without justification.

“ENTERPRISE” status is confirmed in the quote or purchase order. Otherwise, the Client is considered non-ENTERPRISE. The Client may request a change of contractual status at any time. A dedicated point of contact may be designated for ENTERPRISE Clients, if provided in the quote. This enhances long-term engagement.

Unless stated otherwise, these Terms apply in full to both categories. Differences are specified in the relevant clauses.

The Provider guarantees Client Data export at contract end, in a structured, open format (CSV, JSON or equivalent), free of charge except in cases of exceptional volume or specific technical constraints.

The Provider may amend these Terms, particularly if the Service or regulations evolve. Any new version is notified to the Client. For non-ENTERPRISE Clients, the current version is deemed accepted at each renewal.

2 PURPOSE

This contract sets out the Terms under which the Provider grants the Client non-exclusive, non-transferable, and non-assignable access to a SaaS software Service (SAMRoute), for the duration and according to the conditions defined in the Subscription.

- 1 The Service
- 2 Infrastructures
- 3 Location
- 4 Responsibility Limits

2.1 The Service

The Service enables the Client to access a software specialized in analyzing, modeling, and anticipating risks related to transport infrastructure. This software relies on automated data processing, including artificial intelligence algorithms — notably generative AI — to enrich contextual information, generate analytical representations, and support decision-making.

2.2 Infrastructures

The Service relies on two distinct technical infrastructures :

- A high-availability cloud infrastructure, hosted by a third-party provider with enhanced guarantees (redundancy, security, monitoring), progressively deployed as specified in the offer.
- A development infrastructure, used during configuration, prototyping, or customization. No continuous availability is guaranteed ; occasional interruptions may occur (maintenance, connectivity, local constraints).

2.3 Location

Client Data is hosted exclusively within the European Union. The production environment is deployed on OVHcloud data centers located in France (notably in Roubaix and Gravelines), while development and test environments are hosted at the Provider's premises in Ile-et-Vilaine. Any geographic exception requires prior written agreement.

2.4 Responsibility Limits

The Service is provided as-is, with no guarantee of outcome or sector-specific compliance. It is a decision-support tool whose interpretation and use are solely the Client's responsibility. The Provider disclaims any liability for decisions made based on the generated results, including any non-compliance with laws, standards, or frameworks applicable to the Client's sector.

3 ACCESS RIGHTS

This section sets out the conditions under which the Client may access the Service, based on the granted rights, permitted uses, and access methods, including API interfaces.

- 1 License of Use
- 2 Free Access
- 3 Authorized Use
- 4 Access control
- 5 API Access
- 6 Usage Limits
- 7 Monitoring

3.1 License of Use

The Provider grants the Client, for the duration of the contract and subject to full payment of the amounts due, a right to access and use the Service.

This right, which is non-exclusive, non-assignable and non-transferable, allows the Client and its Users to access the Service remotely, via an electronic communication network, under the Conditions defined in this contract.

The Provider may, at its discretion, offer enhanced access levels or customization to meet the specific needs of certain Clients.

3.2 Free Access

The Provider may, at its discretion, grant the Client free, temporary, or limited-feature access to the Service for evaluation, testing, demonstration purposes, or as part of a pilot or beta version. This access is provided “as is,” with no guarantee, continuity, or support obligations, unless expressly stated otherwise.

Such use does not constitute a commercial commitment or implicit agreement for future purchase. It does not grant any additional intellectual property rights or enduring usage rights beyond the defined period.

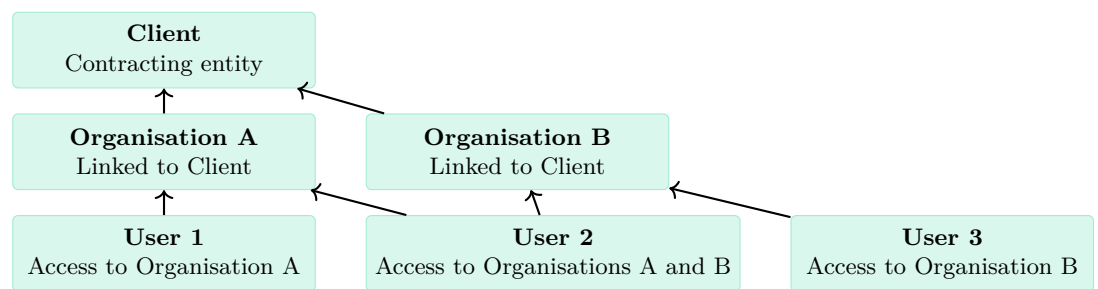
Unless otherwise stated, this access is automatically deactivated at the end of the designated period, unless a commercial subscription is formalized before its expiration.

3.3 Authorized Use

This right of use is strictly limited to the Client’s internal professional needs, excluding any resale, sub-licensing, access by unauthorized third parties — including subcontractors or partners — or use that contravenes applicable laws and regulations. Any use not expressly authorized by this contract is deemed prohibited.

3.4 Access control

The diagram below illustrates the structure of roles between the Client, its technical Organisations, and authorized Users.



3.5 API Access

Access to the Service may include the use of programmatic interfaces (APIs) provided by the Provider, under the conditions set out in the contract. The Provider may restrict usage to reasonable volumes via quotas, time windows, or automatic throttling mechanisms.

In case of repeated overuse or abusive or improper use, the Provider may suspend API access, suggest an upgrade, or apply additional charges in accordance with the applicable offer.

Specific limitations or availability commitments may be defined in a separate agreement (SLA or addendum), upon Client request and Provider approval.

3.6 Usage Limits

The Service includes default technical usage limits, unless otherwise specified or contractually agreed (SLA, addendum). These limits help ensure stability and performance in a shared environment.

By default, per Client : up to 1 GB of files imported via S3, API access up to 10,000 calls per month, and processing capacity appropriate for standard use are included. The Provider may notify of overages and propose an upgrade, or limit access in cases of abuse.

3.7 Monitoring

The Client agrees to ensure compliance with these access Conditions by all its Users, and to promptly inform the Provider of any non-compliant or suspicious use of its account.

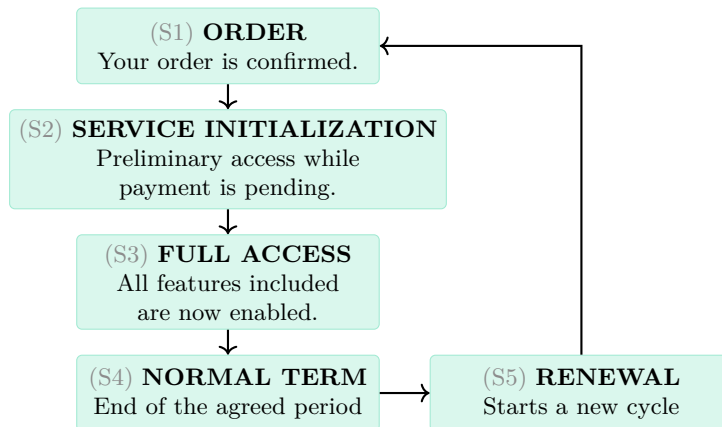
4 CONTRACT LIFECYCLE

This section outlines the main stages of the contractual relationship : start date, duration, renewal, suspension, termination, and contract closure.

- 1 **Process**
- 2 **Start Date**
- 3 **Duration**
- 4 **Renewal**
- 5 **Suspension**
- 6 **Termination by the Client**
- 7 **Early Termination**
- 8 **End of Contract**
- 9 **Change of Control**

4.1 Process

The diagram below shows the stages of the contractual lifecycle, from order to renewal.



4.2 Start Date

The contract takes effect on the start date specified in the purchase order. If no explicit date is mentioned, the Client’s signature date on the purchase order constitutes the “Effective Date”.

4.3 Duration

The contract duration depends on the Client’s category, as specified in the offer or at the time of subscription. If the Client is classified as ENTERPRISE, the contract is concluded for an annual or multi-annual term, according to the Terms set out in the offer. If the Client is non-ENTERPRISE, the contract is of indefinite duration, with monthly billing.

4.4 Renewal

For ENTERPRISE Clients, no tacit renewal applies. The Provider will contact the Client before expiry to propose a new offer. Without explicit acceptance, the contract ends automatically, with no temporary extension or obligation to retain Client Data.

For non-ENTERPRISE Clients, the contract is tacitly renewed on a monthly basis as long as payments are made. It may be terminated at any time under the Terms set out in the section on payment.

4.5 Suspension

If a confirmed or reasonably suspected risk threatens the security, stability, or integrity of the Service (e.g. intrusion attempt, abnormal overload, API abuse), or in the event of persistent non-payment beyond the contractual deadline, the Provider may suspend access to the Service without prior notice. This measure, proportionate to the severity of the situation, will be communicated to the Client as soon as possible. Suspension does not affect the enforceability of any outstanding amounts.

4.6 Termination by the Client

If the Client is classified as ENTERPRISE, it may terminate the contract at any time by written notice (email or registered letter). Termination takes effect thirty (30) days after receipt of such notice. The Provider acknowledges receipt and may, without obligation of result, offer a discussion to support an orderly exit. The Client may receive a refund equal to 70% of the remaining period, calculated pro rata temporis based on the number of unused calendar days between the effective termination date and the end of the initial contractual period. No fees or penalties apply.

If the Client is not classified as ENTERPRISE, the contract is of indefinite duration with monthly tacit renewal as long as payments are honored. The Client may terminate it at any time via the management interface or by simple written notice. To take effect at the end of the current period, the notice must be sent at least fifteen (15) days before the due date. No partial refund is due for any started period.

4.7 Early Termination

In case of a significant contractual breach — technical, financial, or operational, including persistent non-payment — the other Party may notify the breach in writing and request remedy within fifteen (15) calendar days. If not remedied, the contract may be terminated in writing. Compensation is owed only for direct, proven harm within contractual limits.

In the event of a serious, repeated, or irremediable breach — such as infringement of intellectual property or fraudulent use of the Service — termination may be immediate and without notice.

The contract may also be lawfully terminated, without judicial formality, in case of business cessation, insolvency proceedings, or a Force Majeure event lasting more than thirty (30) days. The affected Party shall notify the other as soon as possible.

4.8 End of Contract

If the contract reaches its term or is terminated, access to the Service is suspended on the effective date, with no temporary continuation or automatic extension.

All processing, visualizations, and advanced features cease immediately. Client Data, and any files hosted in object storage (e.g. S3), may be deleted in accordance with the applicable data deletion provisions, with no guarantee of subsequent retrieval.

It is the Client's responsibility to request the export of their Client Data within the timeframes contractually defined for data return, in order to prevent any loss or disruption to their operations.

4.9 Change of Control

In the event of a change of control of the Provider — including merger, acquisition, full or partial asset transfer, or change of majority shareholder — the contract remains valid under the same Conditions, unless stated otherwise. The Client will be informed within a reasonable timeframe. If this change entails a proven risk of non-compliance, conflict of interest, or material loss of guarantees, the Client may terminate the contract in accordance with the applicable termination provisions.

5 PRICING

This section defines the financial Terms applicable to access to the Service. In return for this access, the Client agrees to pay the amounts due to the Provider as specified in the applicable purchase order or commercial offer.

- 1 Changes
- 2 Taxes

5.1 Changes

Applicable prices may be revised by the Provider at the start of each new Subscription period, particularly to reflect changes in operating costs, inflation, or the commercial repositioning of the Service.

For ENTERPRISE Clients, any pricing revision is subject to a new offer or separate purchase order. The new prices only apply after express approval by the Client as part of a renewed contractual commitment.

For other Clients (non-ENTERPRISE) under a monthly Subscription with implicit renewal, any pricing change is notified in writing at least thirty (30) days before it takes effect. The Client may object by terminating the Subscription before that date, without any fee or penalty.

5.2 Taxes

Unless otherwise stated, prices are expressed in euros excluding taxes and are increased by VAT or any other applicable tax on the invoice date.

In the case of a sale to a Client established in another EU Member State with a valid intra-community VAT number, billing is made without VAT, in accordance with the reverse charge

mechanism provided for in Article 283-2 of the French Tax Code. It is the Client's responsibility to declare and pay VAT in their country of residence.

6 PAYMENT

This section sets out the payment terms for the Service, including accepted methods, applicable deadlines, conditions for provisional access, and the consequences of late or failed payment.

- 1 **Methods**
- 2 **Term**
- 3 **Temporary Access**
- 4 **Late Payment**
- 5 **Non-Payment**

6.1 Methods

For ENTERPRISE Clients, payment is made by bank transfer, upon presentation of an invoice, within the deadlines specified in the contract or purchase order.

For all other Clients, payment is preferably made by SEPA direct debit via the Provider's payment provider (Stripe). Other payment methods (credit card, PayPal) may be offered; additional fees may apply. The Client expressly authorizes the Provider to initiate such debits using the banking details provided at subscription and is responsible for keeping them up to date.

No early payment discount applies unless expressly stated in the offer.

6.2 Term

Unless otherwise stated in the validated purchase order or commercial offer, payments are due within thirty (30) calendar days from the invoice issue date. For ENTERPRISE Clients, a period of up to sixty (60) days may be accepted, provided it is expressly stated in the offer or order form. Any period longer than thirty (30) days not previously agreed in writing is not enforceable against the Provider.

6.3 Temporary Access

Full activation of the Service, including all technical capabilities (computing power, storage, advanced features), may be subject to actual receipt of the initial payment. While awaiting payment, temporary partial access may be granted, limited to reading, browsing, and analytics features, excluding data upload (e.g., via S3/Drive).

6.4 Late Payment

Any late payment automatically incurs, without prior notice, late interest calculated at the applicable legal rate, as well as a fixed compensation for recovery costs, in accordance with Article L441-10 of the French Commercial Code. These penalties are payable without the need for a reminder.

6.5 Non-Payment

The consequences of non-payment are described in the section on early termination.

7 CLIENT'S COMMITMENTS

This section defines the Client's contractual commitments, including compliance with the agreement and applicable laws, Client Data management, access confidentiality, and cooperation in the event of an Incident.

- 1 **Contract**
- 2 **Client Data**
- 3 **Credentials**
- 4 **Cooperation**
- 5 **Breach**

7.1 Contract

The Client agrees to use the Service in accordance with the Terms of this contract, as well as applicable laws and regulations. The Client must ensure that access to the Service is strictly limited to its Users, acting within the scope of their professional activities.

7.2 Client Data

The Client is solely responsible for the accuracy, legality, quality, and relevance of the Client Data that it transmits, stores, or processes via the Service. The Client guarantees that such Data does not infringe upon third-party rights or violate applicable laws, especially regarding personal data protection, intellectual property, or public safety.

The Provider does not perform any human moderation or prior review of Client Data. The Client expressly acknowledges that it is solely responsible for verifying the legality and lawfulness of such Client Data.

7.3 Credentials

The Client agrees to keep its access credentials confidential and to ensure their secure use. Any connection to the Service using these credentials is presumed to be made by the Client, unless proven otherwise.

7.4 Cooperation

The Client agrees to reasonably cooperate with the Provider, especially in case of reported malfunction, fraudulent use, or suspected security breach. This cooperation may include providing information useful for understanding or resolving the issue, within a timeframe compatible with the normal operation of the Service.

7.5 Breach

Any breach of the obligations described above may justify temporary suspension of access to the Service, or even termination of the contract, under the Conditions set forth herein. Suspension of the Service shall in no case exempt the Client from its obligation to pay the amounts contractually due under the Subscription.

8 PROVIDER'S COMMITMENTS

This section defines the nature of the Provider's commitments in delivering the Service, the limits of its liability, and the conditions under which a Service Level Agreement (SLA) may be established. It outlines applicable exclusions and reiterates that the Service is a decision support tool without performance guarantees.

- 1 **Best-Effort**
- 2 **Guarantee**
- 3 **Compliance**
- 4 **Monitoring**
- 5 **Logging**
- 6 **Support**
- 7 **Liabilities**
- 8 **Continuity**
- 9 **Evolution**

8.1 Best-Effort

The Provider undertakes to deliver the Service diligently, in accordance with best practices and under a best-effort obligation.

8.2 Guarantee

It does not guarantee the correction of all errors, nor the complete absence of interruptions or defects, especially when the Service relies on shared infrastructure, is under development, or depends on third-party providers (connectivity, hosting, security, etc.).

8.3 Compliance

The Service is provided as described in the validated commercial offer. It is the Client's responsibility to ensure the features meet their operational needs, as stated during contractualization.

8.4 Monitoring

The Provider applies technical monitoring and collects certain usage data to help ensure Service continuity, identify possible improvements, and detect abnormal usage. These operations are conducted for strictly technical purposes, with anonymization or pseudonymization where applicable.

8.5 Logging

The Provider implements logging mechanisms to record access and actions on the Service, including logins, API calls, and data import or modification operations. These logs are retained

for a limited period and used for technical supervision, security, abuse detection, or diagnostics.

8.6 Support

The Provider offers basic support during Business Days through the channels listed in the account or user documentation. It covers access, configuration, and standard usage, excluding customization requests. The Provider aims to respond within a reasonable time, with no guaranteed response time unless contractually agreed. No SLA applies by default. For ENTERPRISE Clients, enhanced support may be included in the offer (dedicated channels, extended hours, named contact, guaranteed response times).

8.7 Liabilities

The Provider's total liability, regardless of cause, is expressly limited to the total amount (excluding tax) effectively paid by the Client in the twelve (12) months preceding the triggering event.

The Provider shall not be held liable for indirect, Incidental, or non-material damages, even if foreseeable — including loss of revenue, profit, data, operations, image, or opportunities.

The Client acknowledges that the Service is a decision-support tool, which does not replace professional judgment or legal/regulatory obligations. The Provider is not liable for the consequences of decisions made by the Client or third parties based on the results produced.

The Provider shall not be held liable in the following situations : improper or diverted use of the Service ; Client's failure to fulfill contractual or regulatory obligations ; unverified decisions based on Service results ; interruptions or outages due to Force Majeure, failures, or third parties beyond its reasonable control.

8.8 Continuity

The Provider implements regular backup and technical monitoring mechanisms to mitigate the risk of data loss. In the event of a critical Incident, it will endeavor to restore the Service within a reasonable timeframe based on the most recent backups. No formal guarantee of recovery time or point is provided unless specifically agreed.

8.9 Evolution

The Provider reserves the right to evolve the Service, including by modifying, adding, or removing certain features, as part of its technical development or commercial positioning. These changes are intended to improve the Service's quality, security, or relevance.

The Provider agrees not to unilaterally remove any major feature that is actively used without at least thirty (30) days' prior notice. In the event of a planned removal, a fallback option, documented alternative, or detailed impact notice may be provided, particularly for ENTERPRISE Clients.

9 AVAILABILITY

- 1 Service Levels (SLA)
- 2 Scope of Commitments
- 3 Maintenance and Scheduled Interruptions
- 4 Suspension for Security Reasons
- 5 Exclusions of Liability

9.1 Service Levels (SLA)

Unless a specific agreement is formally executed between the Parties, no service level commitment (SLA) applies under this contract. No minimum availability is guaranteed by default, and no implied SLA may be enforced.

At the Client's request, a separate SLA may be proposed by the Provider. It defines applicable performance metrics and any contractual compensations, which are exclusive of any other claim or indemnity.

No SLA shall be enforceable against the Provider unless it has been expressly accepted in writing and attached to or referenced in the validated commercial offer.

9.2 Scope of Commitments

The availability commitments provided in this contract, or in a potential Service Level Agreement (SLA), apply only to services operated on the cloud infrastructure.

9.3 Maintenance and Scheduled Interruptions

The Provider strives to ensure continuous access to the Service (24/7), subject to maintenance, Force Majeure, or events beyond its reasonable control. Interventions may be scheduled for updates, patches, or improvements. Except in emergencies, they take place outside business hours (Monday to Friday, excluding holidays) with prior notice to the Client.

9.4 Suspension for Security Reasons

In case of a serious, confirmed, or reasonably suspected threat to the security, integrity, or stability of the Service (e.g., intrusion attempt, misuse of APIs, abnormal system overload, spread of malicious content), the Provider may suspend access to the Service without notice. The Provider will inform the Client as soon as possible of any suspension, specifying the reasons justifying the measure.

9.5 Exclusions of Liability

The Provider shall not be held liable for service interruptions or degradations caused by external factors, including power outages, network failures, Client misconfigurations, or any Force Majeure event.

10 DATA PROTECTION

This section outlines the respective commitments of the Provider and the Client regarding the processing of Personal Data, in compliance with applicable regulations, including Regulation (EU) 2016/679 of 27 April 2016 (GDPR). It details roles, responsibilities, security measures, and compliance mechanisms applied in the context of using the Service.

- 1 Roles (GDPR)
- 2 Public Data
- 3 Client Data
- 4 Processing
- 5 Subprocessors
- 6 Specific agreement (DPA)
- 7 Notification
- 8 Privacy Policy

10.1 Roles (GDPR)

Unless otherwise stated, the Provider acts as a processor under the GDPR, on behalf of the Client, who remains responsible for the processing of Personal Data transmitted, collected, or generated via the Service.

The Provider does not perform any autonomous processing of Client Data without prior written instruction or validation from the Client. The Client remains responsible for informing the data subjects and ensuring the lawfulness of the processed data.

10.2 Public Data

The Provider may index certain information from publicly accessible documents, including names and official roles of signatories acting in an official capacity, for research or consultation purposes by Users. This practice is based on the Provider's legitimate interest and does not involve any linkage with other personal data.

10.3 Client Data

The Client retains full ownership of any Data submitted or collected through the Service. The Provider holds no rights over such data, except those strictly necessary to perform the contract, display results, or generate visualizations and reports. Any other reuse requires the Client's prior written consent.

The Client agrees to process via the Service only Personal Data obtained lawfully, fairly, and transparently, and to inform the concerned Users about its use in accordance with applicable regulations.

The terms for Client Data export and restitution are defined in the section concerning contract termination.

10.4 Processing

The Provider implements appropriate technical and organizational measures to ensure a level of security appropriate to the risks, depending on the environment concerned.

In the production cloud environment, Personal Data is encrypted at rest, stored in secure infrastructures, and subject to traceability, access control, and resilience mechanisms in line with market standards. Access is limited to authorized personnel, and security events are monitored.

In the development environment processing is functionally similar in scope but performed on a distinct infrastructure not intended for final use. Encryption at rest is not systematic, but context-appropriate security measures are applied. Access remains restricted to the Provider's authorized staff, with tailored technical monitoring.

10.5 Subprocessors

The Provider may use third-party services or subcontractors for hosting, storage, payment processing, or audience analytics of the Service, including OVHcloud, Stripe, or Google Analytics. These subprocessors are carefully selected, bound by equivalent confidentiality and security commitments, and operate only within the strictly necessary scope for fulfilling the contract.

No Client Data is transferred outside the European Economic Area without appropriate safeguards in accordance with the GDPR (standard contractual clauses, adequacy decision, etc.).

10.6 Specific agreement (DPA)

A Data Processing Agreement (DPA) may be concluded between the Parties, especially in cases of structured, recurring, or sensitive processing. It will specify the purposes, categories of data, security measures, retention periods, and procedures for exercising rights.

10.7 Notification

In the event of a Personal Data breach (unauthorized access, loss, alteration, etc.), the Provider will notify the Client as soon as possible, to enable them to fulfill their regulatory obligations, particularly toward supervisory authorities or affected individuals.

10.8 Privacy Policy

A separate privacy policy, detailing data processing activities outside this contract or on the website, is available at : www.samroute.com/privacy

11 INTELLECTUAL PROPERTY

This section defines the intellectual property rights related to the Service, associated content, and exchanged data. It distinguishes the rights of the Provider from those of the Client and governs the use of protected elements.

- 1 **Provider Rights**
- 2 **Client Rights**
- 3 **Protected elements**
- 4 **References and communication**

11.1 Provider Rights

The Provider retains all intellectual property rights to the Service, the Service, its software components, interfaces, and Documentation. This includes, unless otherwise agreed, any evolution or improvement made under the contract, including those based on Client suggestions.

Technico-scientific Collateral, as defined in the Definitions section, remains the exclusive property of the Provider, including when derived from processing Client Data.

If a development is commissioned, funded, or co-funded by the Client — especially if it results in Collateral — a written agreement may define reuse, licensing, or co-ownership rights. No rights are transferred without such an agreement.

11.2 Client Rights

The Client has a personal, non-exclusive, and non-transferable right to use the Service for the duration of the Subscription, under the Terms of this contract. This right is strictly limited to internal professional use by the Client and its authorized Users.

Unless agreed in writing by the Provider, the Client shall not reproduce, modify, distribute, or make any part of the Service or Service accessible to third parties (sale, sublicense, API), nor allow indirect access (extraction or reverse engineering).

By exception, the Client may share certain excerpts — notably technico-scientific Collateral — with trusted third parties, provided that attribution, integrity, and non-commercial use are respected. Any external sharing must state : “Analysis generated via the SAMRoute software.”

The Client may internally archive the Collateral for non-commercial use, provided their attribution and integrity are preserved.

Any unauthorized dissemination for commercial, institutional, or public purposes constitutes a material breach. The Provider may suspend access to the Service, terminate the contract without notice, and take appropriate action.

11.3 Protected elements

Protected elements include, in particular, Service technical data, contractual financial Terms, deployment strategies, risk analysis or modeling documents, internal legal guidance, source code, technical documentation, and Client Data not publicly accessible.

These elements fall under the confidentiality framework defined under “Confidential Information”. The associated obligations apply throughout the contract term and for five (5) years following its end, unless otherwise required by law.

11.4 References and communication

Unless explicitly objected to in writing by the Client, the Provider is authorized to mention the Client’s name, logo, and industry sector as a commercial reference in its institutional communication materials (website, presentations, RFP responses, etc.).

Any communication involving direct quotes, reproduction of content, or explicit association with a specific project remains subject to the Client’s prior approval.

12 CLIENT RIGHTS UPON EXIT

This section defines the Client’s rights upon contract termination, including data export, applicable fees, potential transition arrangements, and handling of residual data.

- 1 Export
- 2 Costs
- 3 Transition
- 4 Residual Data

12.1 Export

The Client has thirty (30) calendar days after contract termination to request, in writing, the export of their Client Data. After this period, unless expressly requested otherwise or required by law, the Provider deletes the Data within a reasonable timeframe.

The export is provided in a structured, common, machine-readable format (CSV, JSON, or equivalent). It includes only Client Data, as defined in the Definitions section. Technico-scientific Collateral is excluded unless specifically agreed otherwise.

12.2 Costs

Export is free of charge unless exceptional volume or technical complexity applies — particularly for object-based environments (e.g., S3) involving specific costs. The Provider informs the Client and submits a prior quote. Export takes place only after written approval.

12.3 Transition

During any exit or transition phase, the Parties commit to cooperating in good faith to ensure operational continuity, particularly in the context of a transfer to a third-party solution. The Provider makes every effort to support the Client at each step of their usage, including in case of exit.

12.4 Residual Data

Client Data may temporarily persist in the Provider’s automated backups, without operational use. They are deleted at the end of their standard retention cycle, except in the event of a critical Incident.

13 APPLICABLE LAW AND JURISDICTION

This section defines the contract’s legal framework and dispute resolution procedures, ensuring clear and balanced cooperation.

This contract is governed by French law, to the exclusion of any other legislation.

- 1 Amicable Resolution
- 2 Jurisdiction

13.1 Amicable Resolution

In case of any dispute regarding the validity, interpretation, execution, or termination of the contract, the Parties agree to seek an amicable solution in good faith and within a reasonable timeframe before any legal proceedings.

13.2 Jurisdiction

Subject to mandatory provisions of EU law (Rome I and Brussels I bis Regulations), the Parties agree that any dispute not resolved amicably shall fall under the exclusive jurisdiction of the materially competent courts of Rennes (France), unless otherwise specified in the purchase order.

This jurisdiction clause is agreed between professionals within the meaning of Article 48 of the French Code of Civil Procedure and does not prevent the possibility of contractually adjusting this point if needed.

A SERVICE LEVEL AGREEMENT (SLA)

This annex supplements the General Terms for certain ENTERPRISE Clients. It only applies if expressly attached or referenced in the purchase order.

The fields below are to be completed contractually. Otherwise, no service level commitment applies.

- 1 Contractual Parameters
- 2 Provider Commitments
- 3 Exclusions and Limitations

A.1 Contractual Parameters

Client concerned :

Validity period :

A.2 Provider Commitments

Guaranteed availability :

Support window :

Response time :

A.3 Exclusions and Limitations

No SLA shall be enforceable outside the defined scope or without express written agreement.

B CONFIDENTIALITY

This annex consolidates all contractual confidentiality provisions extracted from the General Terms.

The elements listed below may be distributed across various sections of the contract. This annex facilitates their identification and handling.

In case of inconsistency, the original clause prevails. This extract does not constitute a standalone modification.

- 1 Pre-signature Protection
- 2 Duration and Exceptions
- 3 Extracted Clauses

B.1 Pre-signature Protection

To support open and constructive discussions, the Parties acknowledge that any confidential information shared prior to contract signature — including during demonstrations, technical discussions, or document exchanges — shall be treated with the same level of confidentiality as post-signature obligations.

B.2 Duration and Exceptions

Unless otherwise stated, confidentiality commitments apply throughout the contractual relationship and for a period of five (5) years following its conclusion.

These commitments do not apply to information that is already public, independently known by one of the Parties, or lawfully disclosed by an authorized third party without confidentiality obligations.

B.3 Extracted Clauses

(7.3) The Client agrees to keep its access credentials confidential and to ensure their secure use. Any connection to the Service using these credentials is presumed to be made by the Client, unless proven otherwise.

(8.5) The Provider implements logging mechanisms to record access and actions on the Service, including logins, API calls, and data import or modification operations. These logs are retained for a limited period and used for technical supervision, security, abuse detection, or diagnostics.

(10.1) Unless otherwise stated, the Provider acts as a processor under the GDPR, on behalf of the Client, who remains responsible for the processing of Personal Data transmitted, collected, or generated via the Service.

(10.1) The Provider does not perform any autonomous processing of Client Data without prior written instruction or validation from the Client. The Client remains responsible for informing the data subjects and ensuring the lawfulness of the processed data.

(10.3) The Client retains full ownership of any Data submitted or collected through the Service. The Provider holds no rights over such data, except those strictly necessary to perform the contract, display results, or generate visualizations and reports. Any other reuse requires the Client's prior written consent.

(10.3) The Client agrees to process via the Service only Personal Data obtained lawfully, fairly, and transparently, and to inform the concerned Users about its use in accordance with applicable regulations.

(10.3) The terms for Client Data export and restitution are defined in the section concerning contract termination.

(10.4) The Provider implements appropriate technical and organizational measures to ensure a level of security appropriate to the risks, depending on the environment concerned.

(10.4) In the production cloud environment, Personal Data is encrypted at rest, stored in secure infrastructures, and subject to traceability, access control, and resilience mechanisms in line with market standards. Access is limited to authorized personnel, and security events are monitored.

(10.4) In the development environment processing is functionally similar in scope but performed on a distinct infrastructure not intended for final use. Encryption at rest is not systematic, but

context-appropriate security measures are applied. Access remains restricted to the Provider's authorized staff, with tailored technical monitoring.

(10.5) The Provider may use third-party services or subcontractors for hosting, storage, payment processing, or audience analytics of the Service, including OVHcloud, Stripe, or Google Analytics. These subprocessors are carefully selected, bound by equivalent confidentiality and security commitments, and operate only within the strictly necessary scope for fulfilling the contract.

(10.5) No Client Data is transferred outside the European Economic Area without appropriate safeguards in accordance with the GDPR (standard contractual clauses, adequacy decision, etc.).

(10.6) A Data Processing Agreement (DPA) may be concluded between the Parties, especially in cases of structured, recurring, or sensitive processing. It will specify the purposes, categories of data, security measures, retention periods, and procedures for exercising rights.

(10.7) In the event of a Personal Data breach (unauthorized access, loss, alteration, etc.), the Provider will notify the Client as soon as possible, to enable them to fulfill their regulatory obligations, particularly toward supervisory authorities or affected individuals.

(11.3) Protected elements include, in particular, Service technical data, contractual financial Terms, deployment strategies, risk analysis or modeling documents, internal legal guidance, source code, technical documentation, and Client Data not publicly accessible.

(11.3) These elements fall under the confidentiality framework defined under "Confidential Information". The associated obligations apply throughout the contract term and for five (5) years following its end, unless otherwise required by law.

(11.4) Unless explicitly objected to in writing by the Client, the Provider is authorized to mention the Client's name, logo, and industry sector as a commercial reference in its institutional communication materials (website, presentations, RFP responses, etc.).

(11.4) Any communication involving direct quotes, reproduction of content, or explicit association with a specific project remains subject to the Client's prior approval.

C DEFINITIONS

The following definitions aim to clarify the Terms used throughout this contract. They apply consistently across all clauses, unless otherwise specified.

- 1 The Parties and Their Roles
- 2 Contractual Scope
- 3 Data
- 4 General Terms of Application
- 5 Risks and Exceptions

C.1 The Parties and Their Roles

“Parties” jointly refers to the two signatories of the agreement : the Service Provider and the Client who accepted the offer or subscribed to the Service.

“Provider” (or “Company”) refers to Oriskami SAS, a simplified joint-stock company with a capital of 45 000€, registered with the Rennes Trade and Companies Register under number 892 745 969 (VAT : FR19892745969), with its head office at Parc EDONIA – Bâtiment M, rue des Îles Kerguelen, 35760 Saint-Grégoire, France. The Provider is the entity operating and licensing the Service.

“Client” refers to the legal entity that has subscribed to the Service. The Client is responsible for payment and contractual management of access to the Service.

“User” means any natural person with a personal access environment to the Service, including login credentials, preferences, and permissions, and who is authorized by an Organization to use the Service. A User may be invited to join one or more Organizations, including those outside the original Client’s scope.

C.2 Contractual Scope

“Subscription” refers to the recurring commercial agreement between the Client and the Provider, granting access to the Service under the Terms, durations, frequencies, and pricing defined in the commercial offer or the online subscription interface.

“SaaS” (Software as a Service) refers to a model for accessing remotely hosted software provided to the Client over the internet, without local installation, in a shared or dedicated environment, maintained and operated by the Provider.

“ENTERPRISE” refers to a qualification assigned by the Provider to certain Clients who are part of a direct commercial relationship, structured around an annual or multi-annual commitment formalized through a quote or purchase order.

“Organization” refers to an autonomous usage environment on the Service, linked to a Client Subscription. A single Client may activate several distinct Organizations (e.g., subsidiaries, departments, projects), each with its own Users, settings, and datasets.

“Documentation” means all technical and functional materials provided or made available to the Client, such as user guides, reference manuals, tutorials, or specifications, enabling the understanding and use of the Service.

C.3 Data

“Client Data” refers to any data, document, or content uploaded, entered, annotated, or voluntarily integrated by the Client or its Users via the Service. Technico-scientific Collateral automatically generated by the Service is excluded. The Client retains full ownership of its Client Data. The terms governing the export of such Data are described in the section titled “Terms and scope of data return”.

“Technico-scientific Collateral” refers to results automatically generated by the Service from Client Data, including but not limited to maps, risk scores, representations, indicators, enrichments, or models. These items remain the property of the Provider, unless otherwise stated in writing. They are not included in the default export scope.

“Personal Data” refers to any information relating to an identified or identifiable natural person, as defined under applicable data protection laws, including the General Data Protection

Regulation (GDPR).

“Confidential Information” means any information, regardless of format, marked as confidential or that, by its nature or context, should reasonably be considered confidential. This includes, but is not limited to, technical, commercial, legal, strategic, or financial information exchanged between the Parties.

C.4 General Terms of Application

“Conditions” refers to the set of contractual terms governing access to, use of, availability, limitations, responsibilities, and rights related to the Service provided under this agreement.

“Effective Date” refers to the date on which the contract comes into force, as stated in the purchase order or any other written confirmation from the Provider.

“Business Day” means any calendar day except Saturdays, Sundays, and public holidays in the Provider’s registered office location.

C.5 Risks and Exceptions

“Incident” refers to any actual or suspected event that significantly affects the availability, integrity, or confidentiality of the Service or Client Data, as defined in the relevant clause on service security and availability.

“Force Majeure” means any external, unforeseeable, and irresistible event beyond the reasonable control of the Parties, which prevents either Party from fulfilling all or part of its contractual obligations.

D CONTENTS

1	PREAMBLE	1
2	PURPOSE	2
2.1	The Service	2
2.2	Infrastructures	2
2.3	Location	2
2.4	Responsibility Limits	2
3	ACCESS RIGHTS	2
3.1	License of Use	2
3.2	Free Access	3
3.3	Authorized Use	3
3.4	Access control	3
3.5	API Access	3
3.6	Usage Limits	3
3.7	Monitoring	3
4	CONTRACT LIFECYCLE	3
4.1	Process	4
4.2	Start Date	4
4.3	Duration	4
4.4	Renewal	4
4.5	Suspension	4
4.6	Termination by the Client	4
4.7	Early Termination	5
4.8	End of Contract	5
4.9	Change of Control	5
5	PRICING	5
5.1	Changes	5
5.2	Taxes	5
6	PAYMENT	6
6.1	Methods	6
6.2	Term	6
6.3	Temporary Access	6
6.4	Late Payment	6
6.5	Non-Payment	6
7	CLIENT'S COMMITMENTS	6
7.1	Contract	6
7.2	Client Data	7
7.3	Credentials	7
7.4	Cooperation	7
7.5	Breach	7
8	PROVIDER'S COMMITMENTS	7
8.1	Best-Effort	7
8.2	Guarantee	7
8.3	Compliance	7
8.4	Monitoring	7
8.5	Logging	7
8.6	Support	8
8.7	Liabilities	8
8.8	Continuity	8
8.9	Evolution	8
9	AVAILABILITY	8
9.1	Service Levels (SLA)	8
9.2	Scope of Commitments	9
9.3	Maintenance and Scheduled Interruptions	9
9.4	Suspension for Security Reasons	9
9.5	Exclusions of Liability	9
10	DATA PROTECTION	9
10.1	Roles (GDPR)	9
10.2	Public Data	9
10.3	Client Data	9
10.4	Processing	10

10.5	Subprocessors	10
10.6	Specific agreement (DPA)	10
10.7	Notification	10
10.8	Privacy Policy	10
11	INTELLECTUAL PROPERTY	10
11.1	Provider Rights	10
11.2	Client Rights	10
11.3	Protected elements	11
11.4	References and communication	11
12	CLIENT RIGHTS UPON EXIT	11
12.1	Export	11
12.2	Costs	11
12.3	Transition	11
12.4	Residual Data	11
13	APPLICABLE LAW AND JURISDICTION	11
13.1	Amicable Resolution	12
13.2	Jurisdiction	12
<hr/>		
A	SERVICE LEVEL AGREEMENT (SLA)	13
A.1	Contractual Parameters	13
A.2	Provider Commitments	13
A.3	Exclusions and Limitations	13
B	CONFIDENTIALITY	14
B.1	Pre-signature Protection	14
B.2	Duration and Exceptions	14
B.3	Extracted Clauses	14
C	DEFINITIONS	16
C.1	The Parties and Their Roles	16
C.2	Contractual Scope	16
C.3	Data	16
C.4	General Terms of Application	17
C.5	Risks and Exceptions	17
D	CONTENTS	18