

CLARIFEYE TERMS AND CONDITIONS OF SERVICES

Last update 09/09/2025:

These Terms and Conditions of Services (the “**T&Cs**”) together with the Order Form executed by the Parties constitute a binding agreement (the “**Agreement**”) entered between the Client and CLARIFEYE, a French *société par actions simplifiée* with a share capital of 1 000 €, whose registered office is located at 117 rue de Charenton 75012 Paris, France, registered with the Trade and Companies register of Paris under number 940 450 554 (“**Clarifeye**”). Client and Clarifeye are hereafter individually referred to as a “**Party**” and collectively as the “**Parties**”.

Clarifeye develops and provides an enterprise-grade Software as a Service (SaaS) solution designed to transform document-based information into structured and actionable knowledge.

Subject to the T&Cs and upon execution by the Parties of an Order Form, Clarifeye grants Client access to the Services as follows.

1. DEFINITIONS

“**AI-Generated Outputs**” means results, content or materials generated through the use of Third-Party AI Tool.

“**API**” means any application programming interface provided by Clarifeye for the processing of Client Data by the Solution.

“**Business Days**” means Mondays to Fridays, excluding French public holidays in Mainland France.

“**Business Hours**” means from 9am to 6pm CET during Business Days.

“**Clarifeye Computing Unit**” or “**CCU**” means a unit of computation credit purchased by Client, which can be consumed to execute actions or functionalities made available within the Services, based on their respective usage costs. The consumption of CCUs depends on the nature of the functionalities, in accordance with the applicable pricing model set forth in the Order Form and pursuant to the Documentation.

“**Client**” means the legal entity identified on an Order Form.

“**Client Account**” means the account created on the Platform with admin rights for Client to allow access and use of the Services by Users.

“**Client Affiliate**” means any entity that is, directly or indirectly, controlled by Client. Where “control” means any situation where Client (i) holds the majority of the voting rights in the entity, or (ii) has the power to appoint or remove the majority of the members of the administrative, management or supervisory body of the entity, or (iii) has the power to exercise a dominant influence over the entity by virtue of contractual or legal arrangements.

“**Client Data**” means any and all Incoming Data, Instructions and Outputs.

“**Documentation**” means the User guide, description of the functionalities of the Solution, and, more generally, any other document relating to the use of the Services available from the Platform.

“**DPA**” means Clarifeye’s standard data processing agreement applicable to the use of the Services, as available [here](#), which is attached to the T&Cs by reference.

“**Fees**” means the price due by Client to Clarifeye for the delivery of Services, as set forth in the Order Form. Fees include the purchase price of CCUs as well as any Setup.

“**Incoming Data**” means any data, text, files, documents, images, sound, video, information or content imported into the Platform by any User to be processed as part of the Services.

“**Instructions**” means any commands, prompts, parameters, rules, configurations, settings or other directions specified by Client for the processing of Incoming Data by the Solution.

“**Maintenance**” means any correction and/or update of the Solution made by Clarifeye.

“**Maintenance Period**” means any period during which the Solution is unavailable due to maintenance of the Solution or of the Platform.

“**Order Form**” means the document in the form of a quote or other purchasing document issued by Clarifeye and executed by the Parties for the subscription to the Services. It specifies the Subscription Term, the Metric, the Fees and any other specific terms and conditions mutually agreed upon by the Parties.

“**Outputs**” means any data, results, reports, analysis, compilations or other content generated by the Services from the processing of Incoming Data in accordance with the Instructions, including Processed Outputs and AI-Generated Outputs.

“**Personal Data**” means any personal data within the meaning of applicable law, including the General Data Protection Regulation ((EU) 2016/679).

“**Platform**” means the online platform operated by Clarifeye for the provision of the Services.

“**Security Standards**” means the technical and operational measures implemented by Clarifeye to secure the Platform as set out under Exhibit 2.

“**Services**” means together the supply of the Solution, the Documentation, the Maintenance as well as the Setup.

“**Setup**” means the initial configuration, integration, and technical enablement services to prepare and activate the Services within the Client’s information system environment at the start of the initial Subscription Term.

“**SLA**” means the service levels to which Clarifeye commits for the provision of the Services, as detailed in Exhibit 1.

“**Solution**” means Clarifeye’s proprietary solution, algorithms for machine learning and API, including any updates, revisions, modifications, fixes, additions, and enhancements to it provided through Maintenance.

“**Subscription Term**” means the start date and end date of Client’s subscription to the Services as indicated on the Order Form.

“**Third Party AI Tool**” means any third party tool using artificial intelligence models, machine learning and other probabilistic technology accessible via the Platform for processing Incoming Data.

“**Third Party Service Provider**” means any third party service provider authorized by Client and/or Client Affiliate to access and use the Services on behalf of Client and/or Client Affiliate.

“**User**” means any individual employed by Client, Client Affiliate or a Third Party Service Provider duly authorized by Client and/or Client Affiliate to access and use the Services on behalf of Client and/or Client Affiliate.

“**User ID**” means the personal and confidential login and password, associated to a Client Account, which allow the User to access and use the Services.

2. PURPOSE

The purpose of the Agreement is to set the conditions under which Clarifeye grants to the Client the right to allow Users to access and use the Services for Client’s and Client’s Affiliates internal needs.

3. SUBSCRIPTION AND TERM

Access to the Services requires the prior execution of an Order Form which is governed by the T&Cs.

The Agreement becomes effective on the date of execution of the Order Form and remains in force for the Subscription Term (the “**Initial Term**”). Upon expiration of the Initial Term, the Agreement will be tacitly renewed for additional periods of twelve months (12) months each (each a “**Renewal Term**”) (the Initial Term and any Renewal Term are collectively referred to as the “**Term**”).

4. FINANCIAL TERMS

4.1. Fees. The right to use the Services is granted to Client subject to compliance with the Agreement and payment of the applicable Fees during the Term. Fees are non-refundable, non-transferable and not subject to deduction or set off. CCUs are valid for a period of twelve (12) months from the date of their purchase or until the expiration of the then-current annual Subscription Term, whichever occurs first. Upon expiration of this period, any unused CCUs will automatically expire without compensation or refund to Client. The Client acknowledges that the Services operate on a consumption-based model and that the performance of functionalities within the Services requires the use of CCUs, whose consumption depends on the type and volume of actions performed. The initial pricing applicable to the purchase of CCUs is as set out in the Order Form for the Initial Term. Thereafter, for each Renewal Term, the pricing of the CCUs will be automatically revised annually by seven percent (7%). The Fees are set excluding taxes, Client remains responsible to pay all applicable taxes in force.

4.2. Payment terms. Clarifeye will invoice Client the applicable Fees annually upfront on the effective date of the Agreement and thereafter at each anniversary date

(whether during the Initial Term and/or any Renewal Term), unless provided otherwise in the Order Form. Invoices will be sent electronically. Payment is due within thirty (30) calendar days from the issuance of the invoice and are payable to Clarifeye’s bank account as indicated from time to time. Fees are due regardless of the effective use of the Solution and non-use of CCUs.

4.3. Late payment. In the event of late payment, Clarifeye reserves the right to claim, as of right and without prior formality, late payment interest on a daily basis from the day following the due date until the date of full payment at the interest rate applied by the European Central Bank to its most recent refinancing operation increased by ten (10) points of percentage as well as a recovery fee of forty (40) Euros per invoice, notwithstanding the right to claim for the total amount of the actual recovery costs upon justification. If Client fails to pay the adequate fees more than thirty (30) calendar days after the payment due date, Clarifeye reserves the right to suspend as of right the Services and/or terminate as of right the Agreement without prejudice to any damages that Clarifeye may claim.

5. RIGHT OF USE

In consideration of Client’s compliance with the Agreement, Clarifeye grants to Client, a personal, non-exclusive, non-transferable, and non-sublicensable license allowing Users to access and use the Services for the internal needs of Client and/or or Client Affiliate. Client is not authorized to use the Services to provide services to any third party nor to distribute or market the Services.

6. ACCESS TO THE SERVICES

6.1. Setup. Access to and use of the Services requires a prior Setup performed solely by Clarifeye remotely. The Setup includes, as applicable, the provisioning of a Client Account with access credentials, the customization of settings based on Client requirements, the implementation of data connectors or APIs, support for the integration with Client’s existing systems or third-party tools, as well as one (1) onboarding session for the relevant Users dedicated to the operational deployment of the Services. The Setup does not include the configuration of User’s access rights and provisioning of their credentials which must be done by Client through its Client Account.

6.2. Internet Connection and Registration. Access to and use of the Services is performed remotely through an internet connection to the Platform, at Client’s expense, and prior registration of Client on the Platform to create a Client Account along with the grant of access rights to Users.

6.3. Confidentiality of User IDs. Client is responsible for ensuring that the Client Account and User IDs remain confidential and are not communicated to third parties. Client remains liable for any use of the Services with the Client Account and/or any User ID.

6.4. Compliance by Users. Client is solely responsible towards Clarifeye for the access to and use of the Services by Users as well as for any breach of this Agreement. It is Client’s responsibility to ensure that each User complies with the terms of the Agreement.

7. RESTRICTIONS ON USE

7.1. Technical restrictions. To ensure the stability, performance, and security of the Services for all clients, Clarifeye may implement certain technical parameters as described in the Documentation. Such parameters may include, without limitation, limits on network bandwidth consumption, maximum file upload size, number of concurrent tasks or API calls, and other usage thresholds reasonably determined by Clarifeye. All such parameters are described in the Documentation and may be updated from time to time by Clarifeye in line with technical improvements and industry best practices. The parameters are applied automatically by the Services. Client acknowledges that exceeding such parameters may result in temporary throttling, queuing, or other technical measures necessary to maintain quality of service. At Client's written request, Clarifeye may waive or adjust certain parameters where (i) technically feasible, (ii) justified by a legitimate business use case, and (iii) such adjustment does not materially degrade the Services for other clients. Any such waiver or adjustment will be documented in writing between the Parties. Client agrees not to intentionally circumvent these technical parameters. Clarifeye will act reasonably and in good faith when applying, modifying, or granting exceptions to such parameters.

7.2. Restriction of rights. Client is only authorized to use and allow use of the Services under the terms and conditions expressly set in the Agreement. Clarifeye reserves all other rights. Client undertakes not to (i) copy, make available and/or distribute in whole or in part in any way whatsoever the Services to third parties other than the Users; (ii) access and/or use the Services above the usage limits (including the number of CCUs purchased) without paying the applicable Fees; (iii) assign, sell, lease, lend, sub-license, distribute, outsource or transfer the rights that have been granted to it under the Agreement; (iv) adapt, modify, including for correction purposes, or translate the Services (including underlying software components of the Solution and/or the Platform); (v) disassemble, decompile the underlying software components of the Solution and/or the Platform, perform reverse engineering, or otherwise attempt to discover or reconstitute its source code, except as specifically authorized by applicable law; (vi) alter, destroy or delete notices relating to intellectual property rights or any other reference to Clarifeye's ownership appearing on the Services; (vii) distribute all or part of a software created in whole or in part with the Services; (viii) use the Services for the purposes of benchmarking, or communicate to third parties the results of software performance tests obtained from using the Services.

8. INTELLECTUAL PROPERTY

8.1. Clarifeye property. Clarifeye and its licensors will remain sole owner of all of the material and intellectual property rights attached to the Services. The Agreement does not include any transfer of property to Client except the temporary right of use of the Services granted hereto. Client undertakes not to infringe the property rights of Clarifeye and its licensors.

8.2. Client property. Client and/or Client Affiliates will remain sole owners of Client Data except as provided otherwise with respect to AI Generated Outputs. Client grants to Clarifeye a worldwide, for the duration of the Agreement, license to use Client Data, whether it is supplied by the Client and/or the Client Affiliate, in order to enable their processing and their storage for the performance of the Agreement. Clarifeye undertakes not to perform any training of its proprietary artificial intelligence tool with Client Data.

8.3. AI Generated Outputs. Client acknowledges and agrees that certain functionalities of the Solution may rely on or incorporate Third Party AI Tools. Any AI Generated Outputs produced through the use of such Third-Party AI Tools may be similar to other clients and are provided "as is" and without any warranty of any kind.

For the avoidance of doubt, Clarifeye grants to Client only such rights in and to the AI Generated Outputs as Clarifeye itself lawfully receives from the relevant Third Party AI Tool provider, and no additional rights, licenses, or warranties of any kind are granted or implied. Client shall be solely responsible for determining the suitability of any AI Generated Outputs for its intended purposes and for obtaining any necessary rights, clearances or authorizations relating thereto.

9. PERSONAL DATA

Clarifeye processes Personal Data in accordance with the conditions set out in the DPA.

10. SERVICES

10.1. Hosting of the Services. Clarifeye will host the Services on servers with localization set in the DPA and ensures the remote accessibility of the Platform according to the SLA during the Term except during Maintenance Period or in case of Force Majeure event.

Except in cases of emergency maintenance, Clarifeye undertakes to inform Client in advance by all means (such as by e-mail or via a notification on the Platform) that the Platform will be unavailable. Client acknowledges being informed of the hazards inherent to the internet network and the consequences it may have on the availability and accessibility of the Platform. Clarifeye will in no event be held liable for the temporary inaccessibility of the Services due to Client's hardware or a failure of the internet network.

10.2. Storage of Client Data. Clarifeye will store Client Data imported on the Platform during the Term pursuant to the Security Standards and in accordance with the DPA for the delivery of the Services only, thereafter the Client Data will no longer be available. Notwithstanding the foregoing, Clarifeye's undertaking to implement data back-ups to ensure the remote accessibility and availability of Client Data from the Platform is limited to Instructions and Outputs. Such storage services shall not be construed as relieving Client from taking appropriate measure to back up its Client Data. Clarifeye will not be liable for any loss or destruction of (i) Incoming Data in any way whatsoever, or (ii) Instructions and/or Outputs other than due to failure for Clarifeye to comply with the provisions of the Agreement.

10.3. Maintenance. Clarifeye reserves the right at any time to update and/or change the Solution or the Platform. Such Maintenance will be performed at Clarifeye's discretion. Maintenance includes the provision of updated and additional features of the Solution within the offering purchased by Client.

10.4. Assistance and Technical Support. Clarifeye will use its best commercial efforts to provide assistance to Client by answering during Business Hours reasonable User's questions regarding the use of the Platform sent by e-mail (support@clarifeye.ai) or in the in-app chat. Clarifeye will provide Client with technical support over the Solution as provided under the SLA.

10.5. Additional services. Any Client's request for professional services (other than Setup, such as specific integration with tools not included in the Documentation, specific development, etc.) is outside the scope of the Agreement and will be provided by Clarifeye at Clarifeye's discretion on a case by case basis and according to Clarifeye's standard terms of service.

11. WARRANTIES

11.1. General disclaimer. The Client acknowledges and agrees that the Services are provided on an "as is" basis. Except as set forth herein, Clarifeye expressly disclaims any warranty of infringement, of compatibility, and of fitness for Client's particular purposes. Clarifeye does not warrant that the Services will be error free or that the Platform will operate without interruption. Clarifeye shall hold no liability for any inaccurate Output from the use of the Services. Client expressly agrees to assume all risks inherent to the access to and use of the Services.

11.2. Third-Party rights infringement. During the Term, Clarifeye warrants that it has all the necessary rights or authorizations to grant to Client the limited rights to use the Solution pursuant to the Agreement. In the event of a third party claim brought against Client on the ground that the Solution provided and used in accordance with the Agreement during the Term constitutes a copyright infringement of such third party ("**Third Party Claim**"), Clarifeye agrees to indemnify and hold Client harmless against any damages awarded by a final and binding ruling of a court of competent jurisdiction or agreed to by Clarifeye in a settlement, that arises out of a Third Party Claim provided that (i) Client promptly notifies Clarifeye in writing of any Third Party Claim, (ii) Clarifeye has exclusive control over the defense and settlement of the Third Party Claim, including the right to select legal counsel and to determine the terms of any settlement, (iii) Client cooperates in good faith with Clarifeye by providing, notably, all materials, information and documents in Client's possession or control necessary for such defense, and (iv) Client takes appropriate action to minimize the damages that may result from the Third Party Claim.

Where the Solution is or is likely to be subject to a Third Party Claim during the Term, Clarifeye reserves the right, at its sole discretion, to (i) obtain the right for Client to continue using the Solution, or (ii) modify the portion of the Solution concerned in such a way as to avoid infringement, or (iii) terminate the right to use and access the Solution and, provided that Client complies with the

termination obligations, refund the portion of the prepaid Fees covering the remainder of the Term. This warranty does not apply if the alleged infringement is based on (a) combination or use of the Solution with equipment, product, system, hardware or software not provided or licensed by Clarifeye, (b) use of the Solution other than in accordance with the Agreement, (c) misuse or unauthorized modifications of the Solution, or (d) use of a version of the Solution other than the most current version or failure to implement any new release made available by Clarifeye to remedy a potential third party infringement. The foregoing constitutes the sole and entire warranty granted by Clarifeye to Client under the Agreement and Client shall not be entitled to any other remedy from Clarifeye.

11.3. Client warranties. Client warrants that Incoming Data and Instructions do not (i) violate applicable laws; (ii) contain any virus or malicious code that could harm or corrupt the Platform, (iii) include any information requiring specific regulatory certifications such as but not limited to HIPPA, PCI-DSS, etc, and/or (iv) constitute an unlawful or unauthorized processing of Personal Data. Client undertakes, at its sole cost and expense, to defend and hold harmless Clarifeye from and against any action or claim made by a third party (including without limitation claim of infringement, unfair competition, free riding, Personal Data breach) concerning the use of Client's Incoming Data and Instructions by Clarifeye under the Agreement. Client shall indemnify Clarifeye for all expenses (including lawyers' fees), losses and damages that Clarifeye may incur, together with the amount of any settlement approved by Client and/or compensation for which Clarifeye may be held liable. Clarifeye shall promptly notify Client in writing of any third-party claim in respect of which Clarifeye intends to seek indemnification under the Agreement. Clarifeye shall not admit liability for, or settle, any such claim without the prior written consent of Client.

Client shall retain exclusive control over the defense and settlement of the claim, including the right to select legal counsel and to determine the terms of any settlement, in its sole discretion. Clarifeye shall cooperate in the defense of the claim, including by providing all relevant information, documents and assistance reasonably requested by Client.

12. LIABILITY

Client is solely responsible to ensure that Client Data (other than those hosted by Clarifeye) and its IT systems necessary to access and use the Services are suitably protected.

Clarifeye disclaims all liability for the inaccuracy, loss or alteration of Incoming Data as well as the costs associated with their recovery or in case of indirect damage, including without limitation, loss of income, loss of profits or loss of goodwill resulting from the use of the Services.

Clarifeye is bound by an obligation of means to make the Platform available and provide Services that materially conform to the Documentation. To the extent permitted by applicable law, the liability of Clarifeye in the aggregate is limited to the amount of (i) Fees paid and due by Client under the Agreement for the Setup for any

claim arising from the Setup and/or (ii) the CCUs Fees paid and due by Client under the Agreement during the last twelve (12) months preceding the event giving rise to the claim for any claim arising from the access and use of the Solution. Notwithstanding the foregoing, in case of breach by Clarifeye of its obligations as data processor under the DPA, the aggregate liability of Clarifeye under (ii) above is limited to two (2) times the CCUs Fees paid and due by Client under the Agreement during the last twelve (12) months preceding the event giving rise to the claim. Client's right to claim damages is subject to a limitation period of one (1) year from the occurrence of the event giving rise to the claim.

13. TERMINATION OF THE AGREEMENT

13.1. Termination for non-renewal. Each Party may terminate the Agreement subject to a prior notice to the other Party no later than thirty (30) days prior to the expiration of the Initial or any Renewal Term.

13.2. Termination for cause. Each Party reserves the right to terminate the Agreement in the event of a material breach by the other Party of one or more of its obligations (such as those set out in Articles 4 to 10 and 14). Termination will occur as of right (i) without prior notice (where justified by urgency, in particular due to inappropriate or infringing use by Client of the Services), or (ii) after prior notice sent to the other Party and which remained uncured for a period of thirty (30) calendar days for other breaches, or in the event of liquidation by court order to the full extent permitted by applicable law. Termination will be effective on the day following the expiry of the aforementioned period, where applicable, and is made without prejudice to other rights and remedies available to the Party initiating termination.

13.3. Consequences of termination. In the event of termination of the Agreement, for any reason whatsoever, the rights granted to Client in relation to the access and use of the Services will immediately terminate and Client must immediately cease and have ceased all access and use of the Services by Users.

Termination shall not affect any rights and obligations of the parties that have accrued up to such termination. The provisions of the Agreement that are meant to remain into effect (such as articles 4, 8, 11 to 14 and 17) shall survive termination.

14. CONFIDENTIALITY

Each Party undertakes, with regards to information of a technical (including without limitation the Platform, the Solution, the Documentation), financial, business or otherwise sensitive nature (the “**Confidential Information**”) of the other Party that it may have had knowledge of prior to or during the performance of the Agreement, to (i) keep it strictly confidential and not to copy, communicate or make it available to third parties except to their employees duly authorized, and (ii) not to use it, directly or indirectly, for a purpose other than the performance of this Agreement. Upon termination of the Agreement, each Party undertakes to return or destroy the other Party's Confidential Information in its possession or under its control.

15. BETA FEATURES

Clarifeye may make available to Client certain functionalities of the Services identified as trial, evaluation, beta, or preview features (“**Beta Features**”). Access to and use of Beta Features is optional for Client and is governed by the Agreement, including this article 15 which prevails over any other conflicting provisions. Beta Features are provided “as is”, free of charge, without any warranty of any kind. Clarifeye does not warrant that Beta Features will be free from errors or defects, will operate without interruption, or will be suitable for production use. Unless expressly agreed otherwise in writing between the Parties: (a) Beta Features are excluded from the SLA and any related Service Credits; (b) Beta Features are not subject to the Security Standards or the DPA, except where required by applicable law; (c) Clarifeye has no obligation to provide Maintenance, technical support or updates in relation to Beta Features; and (d) Clarifeye liability in aggregate for any claim arising from the use of any and all Beta Features is limited to five hundred (500) euros. Clarifeye reserves the right to modify, suspend or discontinue any Beta Feature at any time, without prior notice and without liability. Client acknowledges that Beta Features may generate inaccurate or incomplete Outputs. Client shall be solely responsible for its use of Beta Features and the resulting Outputs obtained therefrom.

16. MISCELLANEOUS

16.1. The Agreement constitutes the entire agreement between Client and Clarifeye relating to its subject matter, it supersedes all prior agreements or declarations, whether made in writing or orally. In case of conflicting provisions between the T&Cs and the Order Form, the Order Form will prevail.

16.2. Clarifeye reserves the right to modify the T&Cs at any time subject to prior notice to Client by any means (including e-mails and/or notification on the Platform). The modifications will become effective at the renewal date of the Agreement, it being understood that the Agreement incorporating the revised T&Cs cancels and replaces the existing Agreement (the modified Agreement then becomes the “Agreement”). If Client does not agree to the revised Agreement, it must not access and use the Services and may terminate the Agreement in accordance with article 13.1 above.

16.3. Unless expressly provided otherwise, any notice required under the Agreement must be made in writing and can be delivered by hand or sent by registered letter with acknowledgement of receipt in France or by express mail outside of France, correctly labelled to the address of the other Party as specified on the Order Form. Notices (i) delivered by hand will be deemed to have been made at the time of their delivery, (ii) sent by recorded delivery with acknowledgement of receipt will be deemed to have been made upon their first presentation, (iii) sent by express mail will be deemed to have been made upon their first presentation against signature or (iv) sent by e-mail, where expressly authorized, will be deemed to have been made upon sending to the contact detail of the other Party. Each Party can change its address by sending notice to the other Party. General day-to-day communication may be made by all written means including e-mail.

16.4. Failure of a Party to enforce against the other Party any right it holds under the Agreement shall not be deemed to be a waiver from such Party. Any waiver shall be in writing signed by an authorized representative of such Party.

16.5. Neither Party may be held responsible for a breach of its obligations under the Agreement in the case of force majeure as defined by applicable law and interpreted by the French jurisdictions, including without limitation any governmental decision of any kind, a total or partial strike whether internal or external to the company, a fire, a natural disaster, an act of terrorism, a pandemic, a state of war, a total or partial interruption or a blockage of the telecommunication or electricity networks, an act of computer hacking ("**Force Majeure**").

16.6. The Client expressly authorizes Clarifeye to use and reproduce, for business reference purposes, Client's name, trading name and/or trademark and make reference to the contractual relationship with Client on all promotional vectors used by Clarifeye.

16.7. The Agreement is entered *intuitu personae*, in consideration of Client. Client is not authorized to assign or transfer, for any reason whatsoever (including without limitation internal reorganization, merger, change of control, transfer of assets or other transfer by operation of law), the Agreement to a third party whatsoever, without the prior written consent of Clarifeye. Client expressly acknowledges and agrees that Clarifeye reserves the right to assign or to transfer, in whole or in part, any of its rights or obligations under the Agreement to any third party. The assignment will release for the future Clarifeye from its obligations and liabilities under the Agreement.

16.8. Clarifeye reserves the right to delegate all or part of its obligations to any third-party service provider of its choice.

16.9. If any provision of the Agreement is determined to be void, inapplicable or unenforceable by virtue of law or by any final court ruling, the remainder of the Agreement shall remain in full force and effect.

16.10. Client acknowledges that the Agreement is drafted in English and that it fully understands its meaning and scope without the need for a French translation.

16.11. The Parties expressly agree, as a convention of proof, that the information collected by Clarifeye concerning the use of the Services (including consumption of CCUs) will constitute valid evidence and will be admissible and enforceable between the Parties.

16.12. The Parties expressly agree that affixing their electronic signature to execute an Order Form and/or an amendment to the Agreement constitutes evidence of their consent to the content of the Order Form and/or the amendment to the Agreement so that it is enforceable and legally binding in the same way as if it had been received, executed and stored in a paper-based format. The Parties acknowledge and agree that computer data recorded by a Party and/or the provider of an electronic signature means, as well as the technical information related to the use of the electronic signature means, will prevail between the Parties and constitute valid evidence that are admissible and enforceable in any proceedings.

17. APPLICABLE LAW AND JURISDICTION

The Agreement is governed by French law. In the event of a dispute between the Parties relating to the Agreement that cannot be solved amicably, the Parties agree to the exclusive jurisdiction of the competent courts of Paris (France), notwithstanding plurality of defendants or warranty claims, including urgent or interim proceedings, whether they are summary proceedings or application proceedings.

Exhibit 1 - Service Level Agreement (SLA)

1. Platform availability

Clarifeye will use commercially reasonable efforts to ensure the remote accessibility of the Platform and its availability according to a Monthly Availability Rate of at least 99% in any calendar month during the Term.

The “**Monthly Availability Rate**” means the percentage calculated, per calendar month M, according to the following formula:

$$[(\text{total number of minutes in month M} - \text{total number of Interruption over the month M}) / \text{total number of minutes in month M}] \times 100$$

If Clarifeye fails to meet the Monthly Availability Rate in any given calendar month during the Term, providing Client has been impacted by the failure, Client may claim within thirty (30) calendar days after expiry of the month in question during which the Monthly Availability Rate was not achieved, payment of a Service Credit as follows:

Monthly Availability Rate	Service Credit
Between <99% and ≥98%	5%
Between <98% and ≥95%	15%
<95%	30%

An “**Interruption**” means a situation where the Platform is not accessible or usable by Client, as monitored from Clarifeye’s network, other than due to Availability Exclusions.

No failure by Clarifeye to meet the Monthly Availability Rate will occur if the unavailability of the Solution is caused, directly or indirectly, by (each, an “**Availability Exclusion**”): (a) downtime due to Maintenance Period; (b) any actions of Clarifeye when complying with the request or acting under the direction of Client; (c) access or use of the Solution by Users contrary to the Agreement; (d) Client’s breach of the Agreement; (e) Client’s failure to respond to support requests that require Client’s participation (including in the identification or resolution of Anomaly), as determined by Clarifeye; (f) failures, degradations, or fluctuations in electrical, connectivity, network, or telecommunications equipment or lines, including those caused by Client’s conduct or circumstances beyond Clarifeye’s control; (g) Client’s or a third party’s equipment, software or other technology, not within the sole and exclusive control of Clarifeye; (h) the limitation or suspension of the Solution due to circumstances reasonably considered by Clarifeye as being a threat to the normal operation of the Services (such as use beyond the technical limitations set in the Documentation), the Solution, the operating infrastructure, the facility from which the Services are provided, or the integrity of Client Data (e.g., a hacker or a virus attack); (i) modifications to the Solution not made or authorized by Clarifeye in writing; (j) the unavailability of features of the Solution released for testing purposes (whether expressly identified as such or not); (k) caused by Internet access or related problems beyond Clarifeye’s network; (l) arising from suspension or termination of Client’s right to use the Services; or (m) Force Majeure events.

2. Technical support of the Solution

Clarifeye undertakes to provide Client with technical support in case of an issue affecting the Solution during Business Days. Technical support will be provided through the following address: support@clarifeye.ai. Clarifeye undertakes to make its best commercial effort to meet the following response time objectives:

Type of issue	Response Objective
P1	2 Business Hours
P2	8 Business Hours
P3	2 Business Days

“**Anomaly**” means a malfunction or an error affecting the Solution which has been reported by Client, in accordance with the reporting process set out on the Platform, and has been reproduced by Clarifeye.

“**P1**” means an Anomaly which prevents to process, store or retrieve Client Data in accordance with the Documentation.

“**P2**” means an Anomaly that impairs the functioning of the Solution but does not materially affect the functionality for processing, storage or retrieval of Client Data according to the Documentation.

“**P3**” means an Anomaly that affects a minor functionality of the Solution or its look and feel.

The response time objectives are initial responses from Clarifeye to technical support requests from Client and are dependent upon Client's cooperation and provisions on due time of all the information requested by Clarifeye. Client undertakes to qualify the level of the Anomaly according to the level of severity set above but final and prevailing qualification will be made by Clarifeye after its first assessment. Clarifeye does not commit to meet the objectives or to provide a definitive correction within such response time.

3. Service credits

“Service Credit” is a credit of additional CCUs corresponding to a percentage of the actual CCUs consumed by Client in the calendar month concerned that is credited to Client for a valid claim. In the event no consumption of CCUs occurred during the calendar month due to the unavailability of the Platform, Client may request a flat credit of CCUs equivalent to the average daily consumption calculated over the preceding three (3) months, multiplied by the number of full days of unavailability.

Service Credits are non-cumulative and are calculated monthly, they constitute the sole and exclusive remedy available to Client resulting from Clarifeye's failure to comply with the SLA subject to Service Credits. Client expressly waives its rights to make any other claim for indemnity, such as its right to terminate all or part of the Agreement, to claim for damages or to offset any other Fees payable to Clarifeye.

Exhibit 2 – Security Standards

Clarifeye maintains a comprehensive documented security program under which Clarifeye implements and maintains physical, administrative and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the Services and Client Data.

1. Clarifeye Audits & Certifications

- 1.1. The information security management system used to provide the Services shall be assessed by independent third-party auditors on at least an annual basis for SOC 2.
- 1.2. SOC 2 reports are made available to Client as described in Section 9.2.1.

2. Hosting Location of Client Data

2.1. Hosting Location. The hosting location of Client Data is the production Clarifeye Platform in the region offered by Clarifeye and selected by Client in an Order Form or as Client otherwise configures via the Services at setup time.

3. Encryption

3.1. Encryption of Client Data. Clarifeye encrypts Client Data at-rest using AES 256-bit (or better) encryption. Clarifeye uses Transport Layer Security (TLS) 1.2 (or better) for Client Data in-transit to/from the Services over untrusted networks.

4. System & Network Security

4.1. Access Controls.

4.1.1. All Clarifeye personnel access to the Platform is via a unique user ID, consistent with the principle of least privilege, leveraging single-sign on (SSO) and role-based access controls or a VPN connection, as well as multi-factor authentication and passwords meeting best practice in terms of length and complexity requirements.

4.1.2. Clarifeye personnel will not access Client Data except (i) as reasonably necessary to perform the Services under the Agreement or (ii) to comply with the law or a binding order of a governmental body.

4.2. Endpoint Controls. For access to the Platform, Clarifeye personnel use laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities.

4.3. Separation of Environments. Clarifeye separates production environments from development environments.

4.4. Firewalls / Security Groups. Clarifeye shall protect the Platform using industry standard firewall or security groups technology with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business-required.

4.5. Hardening. The Platform shall be hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in these Security Standards.

4.6. Monitoring & Logging.

4.6.1. Infrastructure Logs. Monitoring tools or services, such as host-based intrusion detection tools, are utilized to log certain activities and changes within the Platform. These logs are further monitored, analyzed for anomalies, and are securely stored to prevent tampering for at least thirty days.

4.6.2. User Logs. Clarifeye also captures logs of certain activities and changes within the Client Account and makes those logs available to Client for Client's preservation and analysis.

4.7. Vulnerability Detection & Management.

4.7.1. Anti-Virus & Vulnerability Detection. The Platform leverages advanced threat detection tools with daily signature updates, which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code (collectively, "**Malicious Code**"). Clarifeye does not monitor Client Data for Malicious Code.

4.7.2. Penetration Testing & Vulnerability Detection. Clarifeye regularly conducts penetration tests and engages one or more independent third parties to conduct penetration tests of the Services at least annually. Clarifeye also runs systematic vulnerability scans for the Platform prior to any update using updated vulnerability databases.

4.7.3. Vulnerability Management. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Services. Upon becoming aware of such vulnerabilities, Clarifeye will use commercially reasonable efforts to address critical and high vulnerabilities within 30 days. Clarifeye leverages the National Vulnerability Database's (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-CERT rating.

5. Administrative Controls

5.2. Personnel Training. Clarifeye maintains a documented security awareness and training program for its personnel, including, but not limited to, onboarding and on-going training.

5.3. Personnel Agreements. Clarifeye personnel are required to sign confidentiality agreements. Clarifeye personnel are also required to sign Clarifeye's information security policy, which includes acknowledging responsibility for reporting security incidents involving Client Data.

5.4. Personnel Access Reviews & Separation. Clarifeye reviews the access privileges of its personnel to the Platform at least quarterly, and removes access on a timely basis for all separated personnel.

5.5. Clarifeye Risk Management & Threat Assessment. Clarifeye security committee meets regularly to review reports and material changes in the threat environment, and to identify potential control deficiencies in order to make recommendations for new or improved controls and threat mitigation strategies.

5.6. Change Management. Clarifeye maintains a documented change management program for the Services.

5.7. Service provider Risk Management. Clarifeye maintains a service provider risk management program for service providers it retains for the provisions of Services that process Client Data. The program is designed to ensure each service provider maintains security measures consistent with Clarifeye obligations in this Security Standards.

6. Physical & Environmental Controls

6.1. Platform Data Centers. To ensure the cloud provider retained for hosting the Platform has appropriate physical and environmental controls over its data centers, such cloud provider shall have a SOC 2 Type II annual audit and ISO 27001 certification, or other best-in-class industry certification. Client Data is not hosted at Clarifeye corporate offices.

7. Incident Detection & Response

7.1. Security Incident Reporting. If Clarifeye becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data (a “**Security Incident**”), Clarifeye shall notify Client without undue delay, and in any case, where feasible, notify Client within 72 hours after becoming aware. To facilitate timely notification, Client acknowledges that the means of notification shall be at Clarifeye reasonable discretion (which may include using the Client-designated email address associated with an Admin roles of the affected Client Account(s))

7.2. Investigation. In the event of a Security Incident as described above, Clarifeye shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

7.3. Communication and Cooperation. Clarifeye shall provide Client timely information about the Security Incident to the extent known to Clarifeye, including, but not limited to, the nature and consequences of the Client Security Incident, the measures taken and/or proposed by Clarifeye to mitigate or contain the Security Incident, the status of Clarifeye’s investigation, and a contact point from which additional information may be obtained. Notwithstanding the foregoing, Client acknowledges that because Clarifeye personnel may not have full visibility to the content of Client Data, it may be unlikely that Clarifeye can provide information as to the particular nature of the Client Data, or where applicable, the identities, number, or categories of affected data subjects. Communications by or on behalf of Clarifeye with Client in connection with a Security Incident shall not be construed as an acknowledgment by Clarifeye of any fault or liability with respect to the Security Incident.

8. Deletion of Client Data.

8.1. By Client. The Services provides Client controls for the deletion of Client Data, as further described in the Documentation.

8.2. By Clarifeye. Subject to applicable provisions of the Agreement, upon the later of (i) expiration or termination

of the Agreement and (ii) expiration of any post-termination “retrieval period” set forth in the Agreement, Clarifeye shall promptly delete any remaining Client Data.

9. Client Rights & Shared Security Responsibilities

9.1. Client Audit Rights. In accordance with the conditions set forth in the DPA regarding Client’s audit rights, upon written request and at no additional cost to Client, Clarifeye shall provide Client, and/or its appropriately qualified third-party representative, access to reasonably requested documentation evidencing Clarifeye’s compliance with its obligations set under these Security Standards in the form of, as applicable, (i) Clarifeye’s SOC 2 audit report, and (ii) architecture and technical overview documentation for the Solution (collectively, “**Audit Reports**”). Audit Reports are considered Clarifeye’s Confidential Information.

9.2. Shared Security Responsibilities. Without diminishing Clarifeye’s commitments in these Security Standards, Client agrees:

9.2.1. Clarifeye has no obligation to assess the content, accuracy or legality of Client Data, including to identify information subject to any specific legal, regulatory or other requirement and Client is responsible for making appropriate use of the Services to ensure a level of security appropriate to the particular content of Client Data, including, where appropriate pseudonymization of Client Data.

9.2.2. Client is responsible for managing and protecting its User roles and credentials, including but not limited to (i) ensuring that all Users keep credentials confidential and not share such information with unauthorized parties, (ii) promptly reporting to Clarifeye any suspicious activities related to Client Account (e.g., a User ID has been compromised) (iii) appropriately configuring User and role-based access controls taking into account the nature of its Client Data.

9.2.3. Client is responsible for the security of any and all third-party tools or applications installed and utilized by Client in conjunction with the Platform.