END USER LICENSE AGREEMENT – YEARLY SUBSCRIPTION

This End User License Agreement govern yearly subscription to the Software Solution and Services.

1. DEFINITIONS

“Applicable Law” refers to the substantive Laws of the State of New York, to the exception of their provisions regarding conflicts of laws, and excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG).

“**Client**” refers to the customer and /or its more than thirty-three percent (33%) controlled subsidiaries and must be a legally registered company in its country of origin.

“**Contract**” for construction and interpretation of this document, refers to the combination of (i) DataDome Quote in its latest version, as sent to and acknowledged by the Client (ii) these General Terms of Sale **and,** wherever relevant (iii) additional documents listed in Article 2 (“Contractual Documents”) below.

“**DataDome**”. refers to Datadome Solutions Inc., a New York corporation having principal offices at 524 Broadway 11th Floor, New York, NY 10012, USA.

“Documentation” refers to the documentation of the Software Solution, accessible at: https://docs.datadome.co/docs as may be updated from time to time.

“**Domain**” refers to all the web pages grouped together in a unique combination of a subdomain, domain name and an extension (or double extension), including the orthographic declensions of the domain names redirecting to the main domain that includes all segments (such as: web, API, mobile API, login, etc.).

“Quote” refers to the proposition offered by DataDome to the Client on receipt of request for Service issued by the Client as per subscription and ordering process detailed in paragraph 3(“Order”) below.

“**Party**” or “**Parties**” refers individually or jointly to DataDome and the Client.

“RegEx” refers to “Regular Expression”, which defines standard search pattern that will be used to provide the Service.

“**Requests**” refers to the base unit processed and invoiced by DataDome. A Request is a call to the DataDome API server from DataDome modules. A Regex allows the Client to filter the types of Requests to be sent over to Datadome’s API server.

“**Service**” refers to the services provided by DataDome in addition to the provision of the Software Solution, as described in the Contract.

“**Software Solution**” refers to the service for monitoring and managing web traffic edited by DataDome and enabling measuring robot traffic and if applicable managing the access rights, as detailed in the Contract.

“**Terms of Use**” refers to the terms of use of the Software Solution, which govern the conditions of use of the Software Solution. They are accessible at (https://datadome.co/terms-conditions/) and can be updated by DataDome from time to time.

“**Terms of Sale**” refers to the present document.

2. CONTRACTUAL DOCUMENTS

By signing, by hand or electronically, these Terms of Sales the Client acknowledges adherence to the Terms of Use, which shall form material part of the Contract.

These Terms of Sale are supplemented by the following appendices to this document which, along with the DPA, express the entirety of the Contract between the Parties:

- Appendix 1: Price List for the subscription to the Software Solution
- Appendix 2: Feature list per offer
- Appendix 3: Service Level Agreement – SLA

In case of conflict or ambiguities between the terms of contractual documentation, precedence amongst element of contractual documentation shall be, in descending order:

- The Quote and Appendix 1 for future Quotes
- General Terms of Sale
- Other Appendices to these General Terms of Sale
- The Data Protection Agreement
- Terms of Use

Protection of Personal Data, and compliance with pertaining regulations, is governed by the DataDome Data Processing Agreement (the **“DataDome DPA”** or the **“DPA”**), which the Parties will sign together with (or without undue delay after) these Terms of Sale, of which it shall form an integral part upon signature.

Any additional commitment or change to the contents of the Contract shall be made by written, mutual agreement in accordance with the provisions of paragraph 22.3, unless the Contract states otherwise.

The Contract covers the entirety of the agreement of the Parties and defines all of their obligations. Previous agreements reached by and between the Parties on services similar to the Services described in the Contract shall be voided and replaced by the Contract upon its signature – or entry into force, whichever is earlier.

Respective documentation issued by either Party, including terms and conditions of purchase of the Client, that are not included in – or expressly referenced by – the Contract shall not apply to the relationship between the Parties.

3. ORDER AND ACCEPTANCE

In order to place an Order, the person representing the Client must have the legal capacity to do so. Requests for Services will be sent to DataDome Customer Success Management to be sent via email. On receipt of such request, DataDome Customer Success Management will issue a Quote for required Services. Any Order placed under this Contract shall be deemed effective on receipt by DataDome Customer Success Management team of a Quote signed by the Client.

4. FINANCIAL CONDITIONS

4.1. Pricing for Service

The Quote issued by DataDome Customer Success Management specifies the conditions of the basic flat rate subscription to the DataDome Software Solution.

The basic flat rate subscription is the level of commitment by the Client for a maximum monthly consumption of Requests as defined in the Price List in Appendix 1.

The Client acknowledges that consumption of Requests in excess of the maximal Requests number permitted under the DataDome Plan subscribed by the Client will be charged in accordance with the Price List presented in Appendix 1.

On the first business day of each month, DataDome will provide a status report of the consumption of Requests over the previous month. If the consumption is found to be greater than the contractual consumption of the basic flat rate subscription, DataDome will send the Client a supplementary invoice according to the provisions detailed below, which will be due by the Client under applicable payment terms provided hereinunder.

4.2. Payment terms

In consideration for the provision of the Software Solution and the Services, the Client will pay the amount indicated in the Quote, in compliance with the terms, schedules and payment method agreed in the Contract and set out in this paragraph. Prices are fixed for the initial Term of the Quote.

All prices are indicated pre-tax: VAT, as well as any other applicable tax or levy due to competent tax authorities under Applicable Law may need to be added at the date of billing if applicable. Where so required by applicable law additional taxes may apply during a same Subscription Period. Any such taxes that are applicable to the sales made under this Agreement are for the Client's account and Client hereby agrees to pay such taxes, provided that Client shall not be responsible for any taxes imposed on, or with respect to DataDome's income, revenues, gross receipts, personnel, real or personal property, or assets.

Any payment due shall be made net and without any deduction. Each invoice issued by DataDome under this Contract is sent as one original copy by electronic means, at the email address provided by the Client. Payment shall be made in the same currency as that contained in the Quote.

Payment of the subscription is due in full at the beginning of the Subscription Period detailed in the Quote. Unless otherwise agreed in the Quote, invoice for the running Subscription Period shall be paid within thirty (30) days of receipt. Payment of supplementary invoices is due at the latest fifteen (15) days from the date of invoice. Payment conditions are specified in the Quote. Payment can be made by bank transfer, automated debit, credit card or by any other payment method accepted by DataDome and specified in the Quote.

4.3. Update of Price List

DataDome may modify prices for Services at any time, including the Price List in Appendix 1. Regardless of the general effective date given by DataDome to its new Price List, it is understood that the Price for Services provided in the Quote shall not change throughout the duration of the Subscription Period.

On expiry of Subscription Period, the Client will be offered an option to renew subscription under the material form of a Quote for a new Subscription Period, which will be based on the updated Price List.

4.4. Delay and disputes

By application of the legal provisions, any delay in payment will result in the application of penalties for overdue payment of one point five (1.5) % of the unpaid invoice, per week, payable without notice from the day following the payment date listed on the invoice.

A flat fee for recovery costs of forty US Dollars (40 USD) if Services provided to the Client by DataDome are invoiced in any other currency than US Dollars (USD) per bill will also be due by the Client. The previously listed fees do not exclude payment of any costs (including but not limited to attorney and court fees), or damages borne by DataDome due to late payment by the Client.

In the event of a payment delay of more than fifteen (15) days, access to the Software Solution may be momentarily interrupted, without notice. In such event, access to the Software Solution shall be restored as soon as the payment shall be proved by the Client. The Contract may also be terminated by DataDome, as detailed in Article "Termination", due to breach of contractual obligations by the Client. Any pending invoices will remain due.

Where the Client declines to pay an invoice (due to material error in the amounts, or because the Client deems the Service has not been delivered in compliance with DataDome's commitments provided in this Contract) the Client shall without delay raise a formal complaint by email, detailing grounds on which invoice has been rejected, to DataDome Customer Success Teams – and the Parties shall discuss in good faith to find a mutual agreement on the situation.

DataDome shall not use its right to suspend the Service as such discussions are taking place.

Where significant or repetitive payment delays were met by DataDome in relationship with the Client, DataDome may demand that all future payments due by the Client, for the remaining of running Subscription Period, are made by credit card or direct debit.

For the avoidance of doubt, suspension of Services that may be decided by DataDome as a result for unjustified delay in payment shall be a partial suspension, only affecting ability of the Client to access and interface with the Software Solution. Processing of Requests sent from Domain protected under this Contract shall continue on an on-going basis until termination or expiry of the Contract is effective.

DataDome will continue processing Data in accordance with the terms of this Contract during discussions surrounding payment of invoices. Therefore, invoices will continue to be issued for any Requests and subscription period started regardless of potential escalation or dispute that may arise.

5. DURATION

Regardless from the date of its signature, this Contract shall enter into force at the date from which Service starts being provided by DataDome, as specified in the Quote.

The Contract will remain into force for the duration of the Subscription Period provided in the Quote. On expiry of the Subscription Period, unless otherwise agreed by the Parties, the Contract shall be renewed tacitly for a further period having the same duration and subject to the terms applicable during the initial Subscription Period.

Subscription can be cancelled at any time by sending an email to accounting@datadome.co. Termination will take effect at the end of the current Subscription Period.

Subject to the exceptions listed in article 7, cancellation of Services during the course of Subscription Period will not result in a refund by DataDome of unused Services.

6. PREREQUISITES

DataDome provides a list of the Software Solution's prerequisites in the Documentation of the Software Solution, which must be complied with by the Client.

DataDome will not be liable if the Client cannot use the Software Solution due to lack of compliance with the prerequisites.

The Client will maintain its internal systems, equipment, and technical environments, to the standard described in the Documentation. DataDome's requirements are listed on: https://docs.datadome.co/docs.

DataDome may update the prerequisites at its discretion but will make its best efforts to notify the Client with sufficient warning.

7. TERMINATION

In the event of a substantial breach by either Party of any of its obligations under this Contract, the non-breaching Party shall provide notice of the breach by sending a formal, registered letter or email with acknowledgment of receipt to the breaching Party. Such notice shall constitute a request to cure the alleged breach.

The breaching Party shall, on receipt of such breach notice, and if possible, prepare, propose, and implement a remedial plan aiming to restore compliance with its contractual obligation within fifteen (15) calendar days (the "**Remedial Period**").

The breaching Party may require the Remedial Period to be extended once, for an additional fifteen (15) days where complexity of actions to be undertaken justifies such extension. The non-breaching Party shall assess such extension request in good faith – but will be left to its reasonable discretion to reject such request in a written notice, which shall provide objective grounds for declining extension.

On expiration of the Remedial Period, or if remediation is not possible, the non-breaching Party may request termination of the Contract, which shall take effect on receipt of the termination notice by the breaching Party – such notice to be sent in a formal, registered letter or email with acknowledgment of receipt.

By way of exception, where the alleged breach involves (i) acts or omission of such reckless nature as to put the business, operations, or reputation of the non-breaching Party at risk, (ii) failure to comply with Confidentiality obligations provided by this Contract **or** (iii) failure to comply with mandatory legal requirements pertaining to collection or processing of Personal Data, the non-breaching Party shall be entitled to demand immediate termination of this Contract. In such case, the non-breaching Party shall serve the breaching Party an immediate termination notice, which shall be sent in a formal, registered letter or email with acknowledgment of receipt detailing the grounds for decision not to allow the breaching Party the benefit of above-mentioned Remedial Period.

By way of exception, where termination of the Contract is requested by the Client due to failure of DataDome to provide Service in compliance with this Contract, DataDome shall refund fees paid in advance for unused period of running Subscription Period.

Where the Contract is terminated for any other cause, the Client shall pay any outstanding invoices and invoices for additional Services, in accordance with payment terms provided in paragraph 4.2, until expiry of the running Subscription Period.

At the effective date of termination or expiry of the Contract, access to the Software Solution will be removed and client data will be deleted by DataDome, in compliance with Article "Reversibility", without liability.

8. DATADOME'S OBLIGATIONS

8.1. General obligations

DataDome warrants and represent that it will provide the Software Solution in SaaS mode and the Services in compliance with the Contract, including Appendix 3 "Services Level Agreement – SLA".

8.2. Related Services

DataDome will provide related Services as follows:

- hosting and related production Services: DataDome hosts the infrastructures necessary for the Software Solution's functioning. DataDome also provides monitoring, technical and application administration and operation of the Software Solution;
- preventative maintenance: DataDome agrees to provide the Client with its expertise in the operation of the Solution in order to anticipate possible malfunctions; and
- corrective maintenance: DataDome agrees to correct any anomaly found in the Solution (application bug, technical problem, etc.), under the terms of Appendix "Service Level Agreement – SLA".

8.3. Evolution

DataDome may develop the Software Solution and related Services, including by adding or adjusting functionalities without incurring additional liability, which is agreed by the Client. It is nonetheless understood that DataDome will take care to avoid such addition or modification having negative impact on the functionalities and performance of the Software Solution.

9. CLIENT’S OBLIGATIONS

The Client undertakes to provide any information and document needed by DataDome to carry out its obligations.

The Client agrees to provide correct and up-to-date information, for the entire duration of the Contract.

The Client undertakes to:

- cooperate fully and in good faith with DataDome. by providing without undue delay such information as DataDome may need to provide the Services efficiently; and
- keep DataDome immediately informed of all difficulties and/or information brought to the Client’s attention likely to have an impact on the performance of the Software Solution; and
- comply with deadlines for which it is responsible when applicable – failing which DataDome shall be automatically excused of subsequent delay or non-compliance of the Service that arose directly of such delay; and
- designate a person who will be the primary point of contact for DataDome; and
- pay all sums due under the terms of this Contract; and
- comply, on an on-going basis with all the terms of this Contract.

Unless specific implementation Services have been agreed to, the Client agrees to follow the Documentation of the Software Solution, in order to implement the Solution on its own Domains.

DataDome will not be liable in case of issues in implementing the Solution to the extent it is attributable to actions or omissions of the Client in spite of unambiguous, written instruction provided (or otherwise made available) by DataDome to the Client.

Any assistance will be provided under the terms of the Quote and Appendix 3 “Service Level Agreement – SLA”.

10. CONFIDENTIALITY

Each of the Parties recognizes that they will need to communicate with one another (as well as with beneficiaries, directors, employees, counsel and subcontractors on a need to know basis – together known as “Authorized Persons”) certain technical, commercial, financial or any other information relating to their respective activities as well as to the Contract and any amendments, and that this information will be delivered in writing, verbally, or by any other means (“Confidential Information”) in the context of the Contract.

This Confidential Information includes, but is not limited to, negotiations and discussions between the Parties relating to the Services any kind of documents or information that is obviously non-public and aims at presenting the activity and internal organisation of each Party, the Service, the Software Solution, and any proprietary data of the Client.

In order to protect the confidential nature of the Confidential Information, each Party agrees under the terms of the Contract:

(i) to keep all Confidential Information in absolute confidentiality and to not disclose it to any third-party (other than to Authorized Persons), except with the prior written permission of the Party owning the Confidential Information concerned
(ii) to use the Confidential Information only in the context of the Contract, and therefore to refrain from any other use, directly or indirectly, in any other purpose or form, for their own benefit or for the benefit of a third party
(iii) to ensure that the Authorized Persons to whom either all or a part of the Confidential Information has been communicated are informed by this Party of the obligations under the Contract regarding Confidential Information
(iv) to return, at the request either Party, all Confidential Information in its possession, and to destroy any copy of any Confidential Information in its possession.

Being understood that the obligations referred to in paragraphs (i) to (iv) above shall not apply to Confidential Information disclosed by one Party which:

- has fallen into the public domain at the time of disclosure or after disclosure, provided that such disclosure is not the result of a breach of confidentiality by the Party having knowledge of the Confidential Information concerned
- was known by the other Party in a legitimate and peaceful manner, before the date on which this Confidential Information was disclosed;
- must be disclosed by the other Party under any Applicable Law or regulation or at the request of any supervisory or regulatory body, administration or tribunal – in such situation the disclosing Party shall, to the extent permitted by Applicable Law (i) inform the disclosing Party on receipt of order to communicate Confidential Information; **and** (ii) provide all reasonable assistance to disclosing Party (at disclosing Party's costs and risks) in legal diligences undertaken to oppose disclosure of Confidential Information;
- is legitimately obtained by the receiving Party via a third party, who in disclosing, breaks no confidentiality obligation;
- is developed autonomously by the receiving Party; or
- is disclosed by the receiving Party with prior written agreement of the Party owning it

The current confidentiality obligation shall apply for the duration of the Contract as well as for a period of two (2) years after expiration or termination of the Contract for whatever reason.

11. INTELLECTUAL PROPERTY

DataDome holds all the intellectual property rights to the Software Solution.

This includes all the specific developments that would be carried out to meet the needs of the Client within the terms of the Contract. The Client is hereby expressly forbidden to carry out any reverse engineering or derivative development works on, or resulting from, the elements of the DataDome intellectual property.

DataDome will defend and indemnify the Client, at its sole expense, against any third-party action or suit against the Client alleging that the Software Solution infringes such third party's intellectual property rights provided that the Client:

- promptly notifies DataDome in writing upon being served a notice by the third party asserting the infringement;
- gives DataDome sole control of the defence and settlement of the Claim (for the avoidance of doubt, a settlement may not be directly adverse to the Client's legitimate interests); and
- reasonably cooperates with DataDome requests for assistance with the defence and settlement of the Claim. DataDome will not be bound by any settlement or compromise that the Client enters into without DataDome's prior written consent.

DataDome obligations detailed above shall not apply to an infringement claim resulting directly from modifications or combination of the Software Solution by the Client or third parties acting on its behalf, that were not expressly authorized, or at least suggested in writing, by DataDome. DataDome remains responsible if the infringement in the Software Solution is caused by third parties acting on its behalf.

THE FOREGOING TERMS STATE DATADOME SOLE AND EXCLUSIVE LIABILITY AND THE CLIENT'S SOLE AND EXCLUSIVE REMEDY FOR ANY CLAIMS OF INTELLECTUAL PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

All trademarks and all logos used by DataDome to identify its products and services, create its marketing documents, and draft its official documents are protected as intellectual property and DataDome is their sole owner.

The Client has no right of copy or use of these trademarks and logos. The Client is not allowed to remove trademarks, logos, copyright notices as well as any intellectual property rights notices, used by DataDome to identify its products.

12. SECURITY MEASURES

DataDome will maintain administrative, physical, and technical safeguards to ensure that the security and integrity of its Software Solution is consistent with industry standard practices.

In this purpose, DataDome has put in place organizational and technical measures to guarantee a level of service that is reliable and secure.

DataDome's market leading expertise on those matters is maintained on an on-going basis through a high level of training of employees and regular control of applied level of security.

For the duration of the Subscription Period, DataDome also undertakes to comply with the following obligations and to ensure compliance by its staff:

- to not make any copies of the documents and information media entrusted to it, except for those necessary for the execution of the Contract; and
- to refrain from using proprietary documentation and information of the Client for any other purposes than those provided in this Contract; and
- to protect Confidential Information in accordance with the provisions of Article 10 ("Confidentiality) above; and
- to take all measures to avoid any misuse or fraudulent use of systems and computer files, including data circulating through the Software Solution; and
- to take all security measures, including hardware, to ensure the conservation and integrity of data, documents and processed information; and
- to destroy, within thirty (30) days of expiry or termination of this Contract for any reason, the Client's data or Confidential information, unless it is legally required to archive it.

13. PRIVACY MEASURES BY DESIGN

DataDome's Technology respects end-user privacy and does not collect any information contained in either the HTTP Post requests body, or the response body, such as but not limited to personal information, email address, credentials, phone number, payment information, information provided when filling forms, details of transactions, etc.

14. PERSONAL DATA

The conditions under which personal data may be collected and processed by the Software Solution are governed by the DPA.

15. REVERSIBILITY

At the latest thirty (30) days after the date of effective termination or end of the Contract, for any reason, DataDome will, at the Client's written request, provide the Client's configuration data on the Software Solution in a standard format such as csv or json.

DataDome can also, subject to a specific quote and payment, provide support for migration to another system which can be done directly with a third-party company chosen by the Client.

16. COMPLIANCE WITH LAWS

Each Party will comply with all Applicable Laws, including but not limited to:

- General Data Protection Regulation.
- U.S. Foreign Corrupt Practises Act of 1977 as well as the French *Loi Sapin II*.
- U.S. laws on imposing export control and trade sanctions, including not being included in a sanctions list, not exporting, or providing services, or participating in any transaction directly or indirectly involving a company subject to export control or trade sanctions.

Client declares that it has not received or been offered any bribe, kickback, illegal or improper payment, gift, or thing of value from any DataDome personnel or agents in connection with the Contract.

17. LIMITED WARRANTIES

EXCEPT AS EXPRESSLY PROVIDED IN THIS CONTRACT AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE SOFTWARE SOLUTION AND THE SERVICES ARE PROVIDED "AS IS", SUBJECT ONLY TO THE COMMITMENTS, REPRESENTATIONS AND WARRANTIES EXPRESSLY PROVIDED HEREIN, AND DATADOME DOES NOT MAKE ANY GENERAL WARRANTIES OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ANY REPRESENTATION REGARDING AVAILABILITY, RELIABILITY OR ACCURACY OF THE SOFTWARE SOLUTION AND THE SERVICES.

DATADOME REPRESENTS AND WARRANTS THAT IT IS THE EXCLUSIVE OWNER OF ALL RIGHTS, ESPECIALLY THE INTELLECTUAL PROPERTY RIGHTS OF THE SOFTWARE SOLUTION, AND THAT THESE RIGHTS HAVE NOT BEEN THE SUBJECT OF A PARTIAL OR TOTAL TRANSFER, NOR OF A RIGHT OF PREFERENCE OR EXCLUSIVITY LIKELY TO PREVENT OR CONTRADICT THE RIGHTS GRANTED UNDER THE CONTRACT. AS SUCH, DATADOME GUARANTEES TO HOLD ALL THE NECESSARY RIGHTS ALLOWING IT TO MAKE THE SOFTWARE SOLUTION AVAILABLE TO THE CLIENT IN THE CONTEXT HEREIN.

18. LIABILITY

EACH PARTY MAY BE HELD LIABLE IF THE OTHER PARTY CAN PROVE THAT THE PARTY HAS BREACHED ITS OBLIGATIONS UNDER THE TERMS OF THE CONTRACT.

BOTH PARTIES ARE LIABLE FOR DIRECT DAMAGES CAUSED TO THE OTHER PARTY DURING THE PERFORMANCE OF THE CONTRACT. IN NO EVENT SHALL EITHER PARTY OR THEIR RESPECTIVE OFFICERS, DIRECTORS, PARTNERS OR EMPLOYEES, BE LIABLE TO THE OTHER PARTY FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE, RELIANCE OR SPECIAL DAMAGES, OR ANY LOSS OF USE, DATA, BUSINESS OR PROFITS, ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE UNDER THIS AGREEMENT.

DATADOME'S ONLY OBLIGATION IS TO PROVIDE THE SOFTWARE SOLUTION AS IS, AND IN COMPLIANCE WITH THE SLA AND THE CONTRACT. DATADOME WILL NOT BE LIABLE IN CASE OF USE OF THE SOFTWARE SOLUTION, BY THE CLIENT, IN A MANNER THAT IS NOT COMPLIANT WITH THE TERMS OF THIS CONTRACT.

IN ANY CASE, THE LIABILITY OF DATADOME, IN THE CONTEXT OF PERFORMANCE OF THIS CONTRACT, IS STRICTLY LIMITED TO THE AMOUNT INVOICED TO THE CLIENT BY DATADOME FOR SERVICE PROVIDED UNDER THIS CONTRACT IN RELATION WITH THE CONTRACT IN THE TWELVE-MONTH PERIOD IMMEDIATELY PRECEDING OCCURRENCE OF THE EVENT ALLOWING THE CLIENT TO ENGAGE DATADOME'S LIABILITY.

UNLESS SUCH LIMITATION IS NOT APPLICABLE DUE TO PUBLIC ORDER REGULATIONS, NO LEGAL ACTION CAN BE BROUGHT BY ONE PARTY ON THE BASIS OF CONTRACTUAL LIABILITY OR ANY OTHER WARRANTY, UNDER THE PRESENT CONTRACTUAL DOCUMENTS, FOLLOWING THE EXPIRY OF A TWO (2) YEAR PERIOD FROM THE DISCOVERY OF THE DAMAGE. THIS PERIOD CAN BE FURTHER LIMITED IF THE STATUTE OF LIMITATION IS SHORTER FOR SUCH ACTION.

19. OUTSOURCING

DataDome agrees to personally carry out the Services. However, a part of the Services may nevertheless be outsourced to third-party suppliers under DataDome's sole control, authority, and responsibility, without exonerating DataDome of its liability towards the Client for the subcontracted Services.

In such case, DataDome shall (i) comply with all applicable provisions of French Law governing relationship with sub-contractors; (ii) arrange and manage payment of sub-contractors without the Client needing to be involved or engaged in the relationship between DataDome and appointed sub-contractor; (iii) warrant on-going compliance of its contractual arrangements with its sub-contractor within the terms of this Contract and all Applicable Law.

20. FORCE MAJEURE

Either Party shall be deemed excused of a failure to uphold its contractual obligations to the extent that such failure is the direct result of an event qualifying as *Force Majeure* under Applicable Law. For construction and interpretation of the provisions set in this paragraph, Force Majeure shall mean acts, events, omissions, or accidents that are both

(i) not reasonably predictable by either Party; **and**
(ii) beyond affected Party's reasonable control.

By way of example, such events may include, without limitation, strikes, lock-outs or other industrial disputes (whether involving the workforce of the Supplier or any other party), failure of a utility service or transport or telecommunications network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or sudden default of a key supplier to a Party.

Force Majeure releases the invoking Party from its contractual obligations only to the extent and for the duration of the event preventing it from fulfilling its commitments. Each Party shall bear the burden of all the costs for which it is responsible, and which are the result of the occurrence of a case of *Force Majeure*.

The Party affected by a case of *Force Majeure* shall immediately notify the other Party and provide all useful justifications. In case the event giving rise to the *Force Majeure* continues for more than 30 (thirty) consecutive calendar days, the Party to which the *Force Majeure* event is opposed to may terminate the Contract immediately without any liability to the other.

No damages or reimbursement may be requested by either Party as a result of termination of this Contract due to a *Force Majeure* event.

21. JURISDICTION

Any dispute or disagreement between the Parties that may not be settled amicably shall be brought to the exclusive jurisdiction of the state or federal court of competent jurisdiction sitting in the City of New York, who shall have exclusive jurisdiction, notwithstanding plurality of defendants or the introduction of third parties, even for summary or conservatory proceedings, by appeal or by petition.

22. GENERAL TERMS

22.1. Compliance with laws

DataDome shall comply, on an on-going basis with all applicable tax and labor legislation and hereby warrants that all its employees benefit from a regular work agreement, including legal, regulatory, and union benefits and rights.

22.2. Insurance

DataDome agrees to underwrite and to maintain for the duration of the contractual relationship one or more types of insurance through a well-known creditworthy company guaranteeing its activity and the responsibilities it may have, or that its potential subcontractors may have, in connection with or in conjunction with the execution of this Contract, covering any damages that might be incurred by the Client arising from, or in connection with, performance of this Contract.

22.3. Update and Amendment of the Contract

The terms and conditions provided in the Contract are binding to the Parties. They may only be updated, adjusted or otherwise modified by means of written amendment.

Such amendment may take the material form of an electronic agreement, which shall be deemed valid and enforceable on completion of process described in paragraph 3 above, **or**, where changes contemplated by the Parties may not be efficiently documented by such process, by means of signature (electronically or in wet ink) of a legal instrument referencing the Contract.

Either Party may initiate amendment process at any time throughout duration of the Contract. A Party to this Contract receiving a change request shall peruse it in good faith and use all commercially reasonable efforts to address reasonable concerns put forward by the other Party.

22.4. Notices

Unless otherwise provided, notices issued by either Party under this Contract shall be deemed to have been validly served on confirmation of receipt of an email.

Such confirmation may be validly provided via automated receipt confirmation, sending of an Order confirmation matching the Order, or even tacitly where subsequent correspondence reference the terms of a given email.

Where the terms of the Contract require a notice to be sent with a formal letter, it shall be deemed to have been served on the date of first delivery attempt.by postal services at the address provided by the receiving Party for correspondence.

The Parties' offices are located as follows:

1. For DataDome: at the address specified in Article "Definitions".
2. For the Client: at the address specified in the Quote.

Unless otherwise provided in the Contract, files, data, messages, and the computer registers archived in each Party's computer systems will be admitted as proof of communications, exchanges, and payments between them.

22.5. Reference

Except with the prior written consent of the Client, DataDome agrees not to prepare or distribute any communication whatsoever, and to make no communication regarding the Contract or related documents and information, regardless of by which means or method.

22.6. No exclusivity

Neither Party shall be limited in its ability to enter into contract with other parties, for services identical or similar to those provided under this Contract.

22.7. No Partnership

The Parties declare that the Contract cannot be considered as an incorporation of a legal person or legal entity, and that their relation is deprived of "a*ffectio societatis*". The Parties also declare that nothing in the Contract shall constitute one Party as an employee, agent, joint venture partner or servant of another.

22.8. Severability

In the event any provision of this Contract is found invalid or unenforceable due to any law, rule or definitive legal ruling, such provision will be considered void. The terms of the Contract that are not directly affected by a cause of nullification shall remain valid and in full force, as if the void provision were no longer part of the Contract.

Where provisions that have been voided result in this Contract losing effectiveness or consideration, the Parties shall meet promptly to discuss alternative provisions to replace those that were voided. The Parties shall discuss in good faith and use mutually their best efforts to uphold the spirit and economic balance of the replaced clause in drafting the replacement provisions.

22.9. Non-Waiver

The Parties reciprocally agree that the fact that one Party elects to waive a contractual right in a given situation shall not be deemed to constitute a precedent, nor to grant any additional right to the other Party.

22.10. Survival

Any provisions in this Contract, which meant by its nature extends beyond the termination or expiration of the Contract, will remain in effect until its full execution and will apply to the Parties' beneficiaries and assignees.

22.11. Titles

In case of interpretation issues between the title of any provision and the provision, the title will be considered non-existent.

22.12. Transfer

Client is not allowed to assign its rights and obligations under the Contract to a third-party, without prior written authorization from DataDome. However, either Party may assign its rights and obligations under the Contract to a third-party in case of merger, acquisition, or other such operations resulting in a change in control of the company under Applicable Law, provided that the transferring Party shall send the other Party a written notice of such assignment.

Appendix 1 – Price List

Price Details:

A list of our current pricing for our services can be found at https://aws.amazon.com/marketplace/pp/prodview-ixqmzzcoyin6m?sr=0-1&ref_=beagle&applicationId=AWSMPContessa.

During the subscription period, the pricing for the Services will be guaranteed for the length of the subscription period.

The Price List is a living document and may be subject to change at any time before your subscription period renews.

In case the amount of requests exceeds the threshold of requests of the Public offers, upon request, DataDome may present a Private offer to the Client.

Appendix 2: Feature list per offer

At the date of signature of this Contract, the Client will be provided, based on chosen options, with the following Features listed here: https://datadome.co/pricing/

The Feature List is a living document and may be subject to change at any time before your Subscription Period renews.

In case the amount of requests exceeds the threshold of requests of the Public offers, upon request, DataDome may present a Private offer to the Client.

Appendix 3 – Service Level Agreement – SLA

1/ DataDome service availability

1.1/ Definitions

"Availability": service availability level

"Unavailability" or "Interruption of Service": the Service is considered unavailable if an automated monitoring system detects a malfunction.

1.2/ Guarantees regarding the availability of DataDome's services

DataDome's Percentage of Availability (A) is determined in the preceding month, and is calculated according to the following formula:

$$A = (MMA – DT) \times 100/MMA$$

Where

The Maximum Monthly Period of Availability (MMA) corresponds to the number of hours per month.
Unavailability (DT) corresponds to the number of hours per month during which the service is not accessible by the Client.
Unavailability (DT) is determined based on the automated detection mechanism.

And Warranted availability is:

Type	Value
Guarantee	**99.9%**

2/ DataDome Technical Support

Technical support is available for ENTERPRISE and CORPORATE plan and only apply if included in the Quote.

2.1/ Definition

"Incident": an event preventing the use of DataDome's services and/or a degradation in DataDome's Services.

2.2/ Technical Support Framework

2.2.1/Scope of technical support

Technical support is available to assist with incidents and questions that go beyond the technical documentation provided.

DataDome is responsible to classify any incident and technical question, at its discretion.

Incidents and technical questions are defined according to the following classifications:

A. Accessibility Issues

a. DataDome causes a major impact on the accessibility of its Clients' websites and/or mobile applications; or
b. DataDome is completely unavailable or inaccessible to its Clients.

B. Configuration Issues

C. Any questions regarding the use of DataDome

2.2.2/ Exclusions from the scope of technical support

DataDome has no obligation for technical support for problems relating to:

1. connection and internet availability
2. connection and the availability of the Client's own infrastructure
3. events that DataDome has no control over or are caused by a "force majeure" event

2.3/ Availability and technical support contact

2.3.1/ Technical support hours

- World: Technical support is available Monday through Friday from 9:00 am to 7:00 pm CET (Central European Time)
- USA: Technical support is available Monday through Friday from 9:00 am to 7:00 pm EST (Eastern Standard Time)

The Client may contact DataDome support by telephone or email (support@datadome.co) to communicate an incident report or to ask a technical question. The Client will have an authorized representative for their requests. This representative with coordinate operational communication between DataDome and the Client.

2.3.2/ On-call personnel outside of technical support hours

Outside of technical support hours, a technical on-call support person is provided by a DataDome-trained employee who will handle the types of incidents outlined in Priority 1. The on-call support person is accessible

- at the following email address: onduty@dataDome.co;

2.4/ Incident submission procedure

2.4.1/ Opening a support ticket

Except in certain situations, the opening of a DataDome support ticket can be done via the following:

- sending an email to support: support@datadome.co

(An acknowledgment of receipt of your ticket is sent to confirm your request.)

2.4.2/ Protocol for opening a support ticket

When opening a ticket by email, it is important to include the following information so we can begin our analysis as soon as possible:

- a description of the incident and requested priority (P1, P2, P3)
- the impact on your service
- a way to reproduce the problem or to see it
- a contact person in case of any questions

2.4.3/ Incident response

Following the receipt of a ticket, an automatic acknowledgement is sent. Regular communications are sent by the support team in order to:

- review the potential issues to analyze/solve the problem
- inform you of the ticket's progress
- inform you of a workaround/resolution of the incident
- request that you to confirm the resolution

When the incident is related to a third party, it is put on standby pending third-party actions.

2.5/ Priority and incident management

Incident reporting priority is defined by DataDome at the time the incident report is written.

The following Priority levels and resolution times shall apply :

Priority level	Definition	Support availability	Target response time	Resolution time (Workaround)

Priority 1 – High	Accessibility issues : - DataDome causes major impact on the accessibility of its Client’s websites and/or mobile applications. - Datadome is completely unavailable or inaccessible to its Clients	On call 24/7 onduty@dataDome.co Monday-Friday 9:00 am - 7:00 pm CET & EST support@datadome.co	2 h	8h (4h)
Priority 2 – Medium	Problems with configuration	Monday-Friday 9:00 am - 7:00 pm CET & EST	1 DataDome working day	2 DataDome working day
Priority 3 – Low	Questions regarding the use of DataDome	Monday-Friday 9:00 am - 7:00 pm CET & EST	1 DataDome working day	4 DataDome working day

2.6/ Resolution notification – Closing out an incident

2.6.1/ Resolved incidents

Depending on the nature of the incident, resolution may be related to:

- a recommendation for using the solution
- the implementation of a workaround
- putting a patch in place
- support in setting up user configuration rules

2.6.2/ Incidents outside the scope

An incident is considered outside DataDome’s scope when its origin is not directly related to the solution. For example:

- integration with a third-party module that’s affecting our module
- Incidents related to your host
- network incidents
- inappropriate use of the application

2.6.3/ Dormant cases

When sending additional questions or requests in order to further the investigation or resolve the incident:

- The ticket moves to pending status.
- If unanswered after 24 working hours, an auto-restart email is sent.
- Without feedback after 24 additional working hours, the ticket is automatically closed.

Regulation (UE) 2016/679, adopted by the European Parliament and Council on April 27, 2016, is applicable as of May 25, 2018 (hereinafter referred to as “the Regulation”).

Since DataDome, acting as Data Processor processes Personal Data within the framework of a commercial contract signed with the Client (the “Contract”) who is the Data Controller, the Parties wish to define the specific obligations of the Data Processor.

As such, the Parties agree as follows:

ARTICLE 1 - PURPOSE OF THE DATA PROTECTION AGREEMENT

The purpose of this Data Protection Agreement is to define the conditions under which the Data Processor agrees to perform the processing of Personal Data on behalf of the Data Controller under the Contract.

In the context of the Contract, the Parties agree to act in compliance with the current regulations applicable to the processing of Personal Data and, in particular, Regulation (UE) 2016/679.

The Data Protection Agreement may be subject to additional conditions in order to take into account any subsequent changes to the applicable texts applying to the Regulation or other applicable laws or regulations, which the Data Processor accepts.

ARTICLE 2 - DEFINITIONS

The following definitions apply to the aforementioned Contract:

"Affiliates": means an entity controlling, controlled by, or under common control with DataDome, that may assist in the provisioning of the Product(s) or Services.

“**Personal Data or Data or PD**”: means any information relating to an identified or identifiable natural person (hereinafter referred to as "the person concerned"); is deemed to be an "identifiable natural person”, a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more specific elements regarding his or her physical, physiological, genetic, psychic, economic, cultural or social identity.

“**Data Controller**”: means the natural person or legal entity, public authority, service or other body which, alone or in conjunction with others, determines the purposes and means of the processing; where the purposes and means of such processing are determined by EU law or the law of a Member State, the data controller may be designated or the specific criteria applicable to his or her appointment may be provided for by EU law or by the law of a Member State.

“**Data Processor**”: means the natural person or legal entity, public authority, service or other body that processes Personal Data on behalf of the Data Controller.

“**Data protection legislation**”: means the California Consumer Privacy Act of 2018 (“CCPA”) and the law of the European Union or any member state of the European Union to which Datadome or Data Controller is subject, which relates to the protection of Personal Data, including without limitation the Regulation and the Directive 2009/136/EC of the European Parliament.

“**Personal Data Breach**”: means any security breach that results in any accidental or unlawful destruction, loss, alteration or non-authorized disclosure of transmitted, retained or otherwise processed Personal Data, or non-authorized access to the Personal Data.

"**Processing**": means any transaction or set of transactions that may or may not be performed through automated processes and applied to the Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, conserving, adapting or modifying, extracting, consulting, using, transmitting, disseminating or any other form of making available, merging or networking, restricting, erasing or destroying.

"**Subsequent Data Processor**": means any Data Processor engaged by DataDome (e.g., the Data Processor) or an Affiliate.

Any capitalized terms used in this Data Protection Agreement and not defined, will have the meaning ascribed to it in the Contract.

ARTICLE 3 - DESCRIPTION OF DATA PROCESSOR PROCESSING

3.1 The Data Processor is authorized to process on behalf of the Data Controller the Personal Data necessary to supply the service(s) defined in the current Contract, and if necessary recalled in Appendix A.

Also defined in Appendix A:

- the nature of the operations performed on the data;
- the purpose(s) of the processing;
- the type of personal data processed;
- the categories of persons concerned; and
- the duration of the processing undertaken by the Data Processor to supply the Service(s).

3.2 In order to perform the services as outlined in the Contract, the Data Controller provides the Data Processor, in Appendix A, with the following necessary information:

- the Data Controller's name and contact information when the processing is performed for multiple Data Controllers
- references for the Data Controller's Data Protection Representative, as defined in Appendix A

This information allows the Data Processor to fill their register in the event that it needs to do so, which must be completed by the Data Processor with any additional information required by law.

ARTICLE 4 - DATA PROCESSOR'S OBLIGATIONS TO THE DATA CONTROLLER

The Data Processor will:

4.1 process the data only as is necessary for the purpose(s) of executing the Contract; and

4.2 process the data in accordance with the Data Controller's documented instructions set out in Appendix A or by any other document accepted by the Parties.

It is hereby specified that, failing that, the Parties agree to define instructions as information provided by the Data Controller to the Data Processor by any means while executing the Contract.

If the Data Processor considers the instructions to be in violation of the Regulation or of any other EU law or law of a Member State relating to Data protection, it agrees to inform the Data Controller immediately.

In the event that the Data Processor is required to proceed with the processing of Personal Data by virtue of a mandatory provision resulting from EU law or the law of a Member State to which it is subject, the Data Processor will inform the Data Controller of this legal obligation prior to processing the Data, except when the applicable law forbids such notice for important public interest reasons.

4.3 In the event of a transfer of Personal Data to another country outside the European Union or to an international organization, the Data Processor shall notice the Data Controller in advance under the process set out in Section 4.7. Data Processor agrees to cooperate with the Data Controller in order to ensure:

- compliance with the procedures for conforming to applicable laws, for example in cases where authorization on the part of a competent supervisory authority would appear necessary; and
- if necessary, the conclusion of one or more contracts to regulate the cross-border flow of Personal Data. The Data Processor agrees in particular, if necessary, to sign such contracts with the Data Controller and/or to obtain the conclusion of such contracts through its Subsequent Processors. To do this, it is agreed between the Parties that the standard contractual clauses published by the European Commission will be used to regulate trans-border Data flows.

4.4 guarantees the confidentiality of Personal Data processed in the context of this Data Protection Agreement.

4.5 will ensure that its employees authorized to process Personal Data under this Data Protection Agreement:

- are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations; and
- Have received the necessary training regarding the protection of Personal Data and how it relates to their handling of the Personal Data and how it applies to their particular duties.

4.6 The Data Processor will take into account, in relation to its tools, products, applications or services, the principles of privacy by design and privacy by default.

4.7 Subsequent Processors
The Data Processor use another sub-processor (hereinafter referred to as the "Subsequent Processor") to conduct certain types of processing. In this case, it will notify the Data Controller in advance and in writing of any planned changes regarding the addition or replacement of other Subsequent Processors.

This notice must clearly indicate the outsourced processing activities as well as the Subsequent Data Processor's identity and contact information, the dates of the outsourcing and the possibility of Personal Data being transferred outside the European Union or to an international organization. The Data Controller has a maximum period of two weeks from the date of the receipt of this information to raise written objections. The Subsequent Processor will only process the Data Controller's Personal Data if the Data Controller has raised no objections during this period. If the Parties do not agree on a solution following objections raised by the Data Controller, the Data Controller will be granted the right to terminate the Contract without penalty.

The Subsequent Data Processor must comply with the obligations of the Contract and the Data Protection Agreement, and to process Personal Data only for the account and according to the Data Controller's instructions. Consequently, the initial Data Processor agrees to sign a written contract with the Subsequent Data Processor - imposing on the Subsequent Data Processor equivalent obligations on the protection of Personal Data as outlined in the Contract and the Data Protection Agreement.

It is up to the initial Data Processor to assure, especially though this written contract, that the Subsequent Data Processor will provide the sufficient guaranties as to the implementation of appropriate technical and organizational measures to ensure that the processing meets the requirements of the Regulation.

If the Subsequent Data Processor does not fulfill his or her obligations regarding the protection of Personal Data, the initial Data Processor remains fully responsible to the Data Controller for the Subsequent Data Processor's performance of its obligations, especially regarding notifications of Personal Data breaches.

4.8 Information of Data Subjects
It is the responsibility of the Data Controller to provide information to data subject at the time of Personal Data collection or, at the discretion of the Data Controller, to request the Data Processor, at the time of Personal Data collection, to provide the information relating to the Personal Data that it processes to data subjects. In this latter case, the content and format of the information will be subject to prior written approval of the Data Controller prior to any Personal Data collection.

4.9 Exercise of the rights of Data Subjects

As far as possible, the Data Processor shall assist the Data Controller in fulfilling its obligation to respond to requests for the exercise of data subjects' rights under the Personal Data Legislation, namely: the right to access, correct, erase, oppose, the right to restrict processing, the right to Personal Data portability, the right to not be subjected to automated decision making (including profiling).

When data subjects exercise their rights with the Data Processor, the Data Processor shall send these requests via email to the person designated by the Data Controller in Appendix A or communicate by any other means that the Data Controller chooses. The Data Processor can respond directly to the data subject's request only at the Data Controller's instruction.

4.10 Notification of Personal Data breaches

A breach of Personal Data means any security breach that results in any accidental or unlawful destruction, loss, alteration or non-authorized disclosure of transmitted, retained or otherwise processed Personal Data, or non-authorized access to the Personal Data.

When a Personal Data breach has taken place, the Data Processor agrees to carry out any necessary investigations on the breaches of the rules of protection in order to remediate as soon as possible and diminish the impact of said breaches on data subjects.

The Data Processor notifies the Data Controller of all Personal Data breaches as soon as possible and, in any case, within forty-eight (48) hours after having become aware of it. This notification shall be accompanied by all relevant documentation enabling the Data Controller, if necessary, to notify the relevant supervisory authority of the breach.

The Data Processor shall be informed that in the event of a notification of a Personal Data breach by the Data Controller to the competent supervisory authority, the notification shall contain at least:

(i) a description of the nature of the Personal Data breach including, if possible, the categories and the approximate number of people affected by the breach and the categories and approximate number of Personal Data records concerned.

(ii) the name and contact information of the data protection officer or other point of contact from whom additional information can be obtained.

(iii) a description of the likely consequences of the Personal Data breach.

(iv) a description of the measures taken or how the Data Controller proposes to remedy the Personal Data breach, including if necessary, measures for mitigating any negative consequences.

If, insofar as it's not possible to supply all the information at once, it may be communicated in increments without undue delay. In any case, the Data Processor agrees to inform the Data Controller of its investigation into the rules of protection breaches which led to the Personal Data breach, the development and consequences of the breach, as well as the measures taken or planned to reduce the impact of the identified breaches, and this on a regular basis.

The Data Processor agrees to actively collaborate with the Data Controller in order for them to meet their regulatory and contractual obligations. Only the Data Controller can inform the relevant supervisory authority of the Personal Data breach and provide information on this breach to the persons concerned; the Subcontractor therefore refrains from making such notification and communication.

4.11 Data Processor assistance in complying with the Data Controller's obligations

The Data Processor will assist the Data Controller in performing Data Protection impact analyses that the Data Controller decides to perform.

The Data Processor shall assist the Data Controller in the preliminary consultation of the supervisory authority following the completion of impact analyses.

4.12 Security Measures

Without prejudice to the provisions in the body of the Contract, the Data Processor shall implement all appropriate technical and organizational measures to protect Personal Data, taking into account the state of knowledge, implementation costs, nature, scope, context and the purposes of the processing as well as the risks, whose degree of probability and severity may vary to the rights and freedoms of natural persons in order to guaranty a level of security appropriate to the risk.

The Data Processor especially agrees to take all necessary precautions with respect to the nature of the Data and the risks encountered by its processing in order to preserve the security of the Data files and especially the prevention of any corruption, alteration, damage, accidental or unlawful destruction, loss, disclosure and/or access by any unauthorized third parties.

In particular, the Data Processor agrees to ensure total separation between the Data Controller's Data and the Data Processor's other clients via a reasonable and physical or logical separation.

The means implemented by the Data Processor for ensuring the security and confidentiality of the Data especially includes the following measures, to be outlined in Appendix A, such as:

- the encryption of Personal Data
- the means of ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- the means of restoring access and availability of Personal Data within the appropriate/defined time limits in the event of a physical or technological mishap
- a procedure for regularly testing, analyzing and evaluating the effectiveness of technical and organizational measures to ensure safe processing

The Data Processor agrees to maintain these measures throughout the entire Contract period and to immediately inform the Data Controller of any failures that may impact the Data Controller's Data.

In all cases, when any of the methods for ensuring the security and confidentiality of the Personal Data and files are changed, the Data Processor agrees to replace them with superior methods. No change shall lead to a lessening of the security level.

4.13 Data return and destruction

Upon termination of the Contract the Data Processor agrees, if applicable:

- to return all Personal Data and files to the Data Controller in a useable format and within the specific conditions specified by the Data Controller.
- to send the Personal Data to the Data Processor designated by the Data Controller and then,
- to destroy all Personal Data and manual or computerized files containing the information collected within a timeframe of two (2) months after its return, in order to allow the Client to have the necessary time to verify that the returned Data is usable and readable, unless stipulated otherwise by community law or the law of a Member State of the European Union applicable to the processing covered by this agreement.

The return must be accompanied by the destruction of all existing copies in the Data Processor's information systems. The Data Processor will attest to it in writing following a written request from the Data Controller.

4.14 Data Processor's data protection Officer

The Data Processor's data protection officer is Mr. Romain CATALA, legal Manager & DPO (contact information: privacy@datadome.co).

4.15 Register of processing activity categories

The Data Processor declares that it keeps a written record of all processing activity categories performed on behalf of the Data Controller, including:

(i) the name and contact information of the Data Controller on whose behalf they are acting, any Subsequent Data Processors and, where applicable, the Data Protection officer.

(ii) the processing categories performed on behalf of the Data Controller.

(iii) where applicable, Personal Data transfers to a third country or international organization, including the identification of the third country or international organization and, in the case of transfers referred to in Article 49, paragraph 1, sub-paragraph 2 of the Regulation, documents proving the existence of appropriate safeguards.

(iv) to the extent possible, a general description of technical and organizational security measures including, among others, as required:

- the encryption of Personal Data;
- methods for ensuring the ongoing confidentiality, integrity, availability and resilience of the processing systems and services;
- methods for restoring the availability of Personal Data and timely access to this data in the event of a physical or technical incident; and
- procedures for regularly testing, analyzing and evaluating the effectiveness of technical and organizational measures for ensuring processing security.

4.16 Documentation

The Data Processor shall supply the Data Controller with the necessary documentation for demonstrating compliance with all obligations under this Data Protection Agreement.

ARTICLE 5 - DATA CONTROLLER'S OBLIGATIONS TO THE DATA PROCESSOR

The Data Controller agrees:

- to supply the Data Processor the data referred to in Article 3 above in these Data Protection Agreement;
- to provide written documentation of all instructions regarding the Data Processor's processing of Data;
- to ensure in advance and throughout the duration of processing that the Data Processor complies with the obligations outlined in the Regulation; and
- to oversee processing.

ARTICLE 6 - COOPERATION IN THE EVENT OF AUDIT

In the event of audit by a competent authority, the Parties agree to cooperate between themselves and with the supervisory authority.

In the event that the audit carried out concerns only the processing implemented by the Data Processor acting as the Data Controller, the Data Processor shall be responsible for the audit and shall refrain from communicating or reporting the Data Controller's Personal Data

In the event that the audit carried out at the Data Processor's premises concerns the processing operations performed in the name and on behalf of the Data Controller, the Data Processor agrees to immediately inform the Data Controller and to make no commitment on his or her behalf.

In the event of audit by a competent authority on the Data Controller's premises, including the services provided by the Data Processor, the latter agrees to cooperate with the Data Controller and to provide him or her with any information required or which would be necessary.

7. TERM AND TERMINATION

This Data Protection Agreement will remain in full force and effect so long as:

(a) the Contract remains in effect; or

(b) the Data Processor retains any of the Personal Data related to the Contract in its possession or control (Term).

Any provision of this Data Protection Agreement that expressly or by implication should come into or continue in force on or after termination of Contract in order to protect the Personal Data will remain in full force and effect.

APPENDIX 5 – DATA PROCESSING

1 - DESCRIPTION OF PROCESSING

1 - The Data Processor is authorized to process the necessary Personal Data on behalf of the Data Controller in order to:

Provide the services as defined by this Contract:
DataDome, publisher of a SaaS Software Solution for the tracking and managing of web traffic in order to track robot traffic and, where appropriate, to manage access rights and, where necessary, to block malicious traffic.

The nature of operations performed on the data is as follows:

- DataDome analyzes the IP addresses of visitors to the client's sites and mobile applications in real time as part of a robot traffic detection service by the Software Solution known as DataDome.
- DataDome stores and processes the Administrator data (Client users) that is required for access to the DataDome Dashboard (authentication).

Purpose of the processing:
The DataDome software solution analyzes web traffic accessing the client's sites and APIs in order to classify it, identify Bot traffic and, where necessary, to block it.

Types of Personal Data Processed include:

- Visitors to the Client's site:
    - IP addresses for connecting Visitors to the Client's site
    - cookie session Identifiers for visitors to the Client's site (Appendix 5)

- Administrator data (Client users)
    - first name, last name
    - work email address

Data Subject categories include:

- Visitors to Client's site
- the Data Controller's employees having access to the DataDome Dashboard (referred to as "Administrators")

The processing duration is:
The duration of the Contract plus the duration of archiving as provided for in the Contract and up until the destruction of the data by the Data Processor.

For the purposes of the robot detection and blocking service, DataDome collects and stores for 30 rolling days (with automatic management of deletion beyond 30 days) the IP addresses as well as information related to the browser (user agent, set language, screen resolution etc.)

Data from actions performed by the Administrators are subject to a daily backup and will be deleted within fifteen (15) days of the expiration of the Contract for whatever reason.

2. Authorized Subsequent Processors

The hosting Subsequent Processors vary depending on the Client’s location. More information can be found in the Security Assurance Plan.

Provider	Mandatory / Optional	Service	Location of data
Amazon Web Services	Mandatory	Processing / Storage	USA
Google Cloud	Mandatory	Processing / Storage	USA
OVH	Mandatory	Processing	USA
Vultr	Mandatory	Processing	USA

2 - INSTRUCTIONS

The Data Processor agrees to process the Data Controller’s Personal Data according to the Data Controller’s documented instructions below or to the provisions of this contract (see appendices) or any other document accepted by the Parties.

3 - CONTACT PERSON DESIGNED BY THE DATA PROCESSOR

In the event that a data subject exercises his or her rights with the Data Processor, the latter will forward these requests to the Data Controller, upon receipt, to the following address for the contact person designated by the Data Controller, in this Appendix or separately.

4 – METHODS PUT IN PLACE TO ENSURE THE CONFIDENTIALITY AND SECURITY OF THE DATA PROCESSED

For the purposes of the robot detection and blocking service, we analyze incoming traffic on our clients’ sites: IP addresses, headers and javascript rendering. The data that we collect and store is protected using modern and high-performing security standards:

- For clients choosing to connect the DataDome module to the DataDome API server hosted by Online, the infrastructures on which the DataDome software solution is hosted are located in France. All the data is stored in separate indexes and shared across multiple Tier 3 European data centers.
- The DataDome modules, installed on clients’ web servers, create a persistent connection with our API servers which execute the DataDome software solution.
- Information exchanged between the module and the API servers are secured using an HTTPS connection. Authentication is done through an API key identifying the client account.
- Access to the administration Dashboard is protected by an authentication based on a login/password on an HTTPS connection. Calls to the REST API in the Back Office are secured by an OAuth2 authentication delegation.
- Communication between DataDome’s internal components, when they are not in an intra-data center trust network, are encrypted (TLS or Ipsec VPN).

Appendix 6
Cookie Management

The solution offered by DataDome, the subject of this contract, implies the use of cookies.

DataDome agrees to comply with all legal and regulatory provisions or recommendations of the supervisory authority, as in effect, namely in particular: Directive 2009/136/EC and Article 32-II of the amended law of January 6, 1978 as well as the provisions of the CNIL 2013 378 deliberation of September 17, 2020 regarding cookies.

Cookies deposited as part of the DataDome service are similar to "session identifiers" and "load balancing" cookies, since through the identification of characteristics linked to a user, it allows the DataDome module installed on the client's server to either grant access to the website or present to the "user-robot" a page containing a captcha, allowing it to confirm the access ban to the customer's website. DataDome cookies:

- do not require the user's/visitor's consent;
- are valid for 12 months; and
- are first-party cookies linked to the Client's domain name. Data collected is specifically used on the Client's behalf.

Specifically, DataDome agrees:

- that for all types of cookies deposited, whether on behalf of the Client, for their own use or for the use of a third-party publisher, they will not exceed the maximum duration of thirteen (13) months.
- to deactivate or disable cookies upon expiration of the contract for whatever reason, regardless of the cause and the author.
- that cookies deposited shall collect only the data defined between the Parties, and overall adhere to the criteria in this table:

Cookie name	Purpose (if more than one purpose applies to the same cookie, all purposes must be indicated)	Publisher and/or indication on behalf of which publisher (example governed) the cookie is deposited	Valid for:	Data collected:
DataDome Cookie	Technical cookie session ID	DataDome	12 months	ID session

- to obtain the Client's prior and express agreement to any modification of cookies deposited (e.g., purpose, data collected, publishers on whose behalf the cookies are deposited) as specified in the above table. DataDome will update the above table.
- to comply with the provisions of Article 32-II of the Data Protection Act.
- to only use the following technologies in fulfillment of the contract:
  - those which are reliable, safe and state-of-the-art
  - those which can technologically and easily manage the deletion of cookies

    - those which only allow the collection of data as identified by the Parties, and which generally comply with the criteria outlined in the table above
- to not collect data other than that which is specified, it being understood that the Client is free to collect other data on his or her own initiative via the technology made available to her or her.
- to not use cookies for any other purpose other than what is outlined in the Contract.
- to not include in the technologies provided or used, any virus or other malicious element that could corrupt the security of the data or digital media from which it is distributed, or to collect data (personal or not) other than what is defined between the Parties.