END USER LICENCE AGREEMENT

This End User Licence Agreement (this “EULA”, together with the Order(s), all appendices to this EULA, and the Terms of Use defined below, this “Agreement”) governs Client’s subscription to the Services.

1. DEFINITIONS

“**Affiliate**” refers to the Client’s controlled subsidiaries, legally registered in its origin country.

“Agreement” for construction and interpretation of this document, refers to the combination of (i) the Order(s) signed by the Client, (ii) the Terms of Use (iii) this EULA and (iv) its Appendices.

“**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).

“**Authorized Users**” refers to the Client’s or an Affiliate’s individual employees, directors, agents, independent contractors, who are accessing or using the Service under the rights granted to Client pursuant to this Contract.

“**Client**” refers to the legal entity signing the Contract.

“**Client Data**” refers to any data, information, or material that is transmitted by the Client to DataDome in connection with Client’s use of or access to the Service or generated by the Workspace for Client.

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

“DataDome API” DataDome Application Programmatic Interface (DAPI) is a set of definitions, URL endpoints, and HTTP-based protocols for building and integrating with DataDome’s application software.

“**Documentation”** refers to the documentation related to the Service, accessible at: https://docs.datadome.co/docs as may be updated from time to time.

“**Domain**” refers to Client’s 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.).

“**Fees**” are defined in Article 6.

“Module” a versioned release of the Workspace that defines a means of interface between Client’s infrastructure and DataDome’s distributed data collection and processing engine.

“Open-Source software” refers to a software with its source code made available pursuant to a license by which, at a minimum, the copyright holder provides anyone the rights to study, change, and/or distribute the software to anyone and for any purpose.

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

“**Plan**” refers to the DataDome plan subscribed by the Client (Business, Corporate, Enterprise, Enterprise Plus, as such terms may vary from time to time). The Plan chosen impacts the number of Requests available to Client, and the Services provided. The Services features for each Plan are provided in Appendix 3.

“Order” refers to an ordering document signed by Client and the Reseller Partner which defines the specific terms of the Client’s Subscription to the Services.

“**Requests**” refers to the base unit processed and invoiced by DataDome. A Request is a call to the DataDome API server. The Client subscribes to a Plan that includes a certain number of Requests. Any Request used in addition to this number is an “**Additional Request**”.

“Reseller Partner” refers to a partner of DataDome that is authorized to resell the Services to Client.

“**Service(s)**” refers to the services provided by DataDome to Client, including the provision of the Workspace, hosting of the Workspace etc. The Services can include different types of protection (e.g. Bot Protection, Online Fraud Protection etc.).

“**Subscription**” refers to the purchase of Services by Client according to a Plan, for a number of Workspaces and for a certain Subscription Period (all these elements being defined in the Order).

“**Subscription Period**” refers to the duration of the Services as provided in an Order.

“**Terms of Use**” refers to the terms of use of the Workspace by individual users. They are accessible when registering/logging in the Workspace for the first time, and must be accepted by all Authorized Users, and can be updated by DataDome from time to time. For reference, these are accessible here: https://datadome.co/terms-of-use/.

“**EULA**” or “**End User Licence Agreement**” refers to the present document.

“**Workspace**” refers to the DataDome’s proprietary SaaS solution to which Client has access when logging in to https://app.DataDome.co/dashboard/login which consists of a user interface for the reporting of security events occurring within the scope of defined Domains and endpoints.

2. ACCEPTANCE OF AGREEMENT

Upon execution of an Order between Client and Reseller Partner, Client and DataDome will be deemed to have entered into and be bound by this Agreement.

This Agreement is effective upon the effective date set forth in the Order ("Effective Date"). Client's use of and access to the Service is governed by this Agreement.

In order to place an additional order for Services (Plan upgrade, new Services features, additional Workspaces…), the person representing the Client must have the legal capacity to do so. Client will send the request to DataDome Customer Success Management via email. On receipt of such request, DataDome Customer Success Management will issue an Order for required Services, to be fully signed by the Client in order to become effective.

This Agreement consists of the provisions to the present document and the following appendices which form an integral part of the Agreement:

- Appendix 1 : Data Protection Agreement
- Appendix 2 : Service Level Agreement
- Appendix 3: Business model and feature list per Plan

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

- The Order(s)
- The Data Protection Agreement
- EULA and other appendices
- Terms of Use

3. DATADOME'S SERVICE TERMS

3.1 Workspace License Terms

a. Subject to the terms and conditions hereof, DataDome grants Client a non-exclusive and non-transferable license for the Subscription Period, to use the Workspace or several Workspaces, up to the number of Requests defined in the chosen Plan. Access to one Workspace is granted for 30 endpoints, 50 Authorized Users and 3 Domains.

b. The grant of the license described in the present section is conditioned upon Client's ongoing compliance with its obligations under this Agreement, the Order, the Terms of Use, and the Documentation, and especially the pre-requisites set out below.

c. Authorized Users are required to choose a password and username to access the Workspace. Username shall be nominative and not generic. DataDome will block access to any generic username. Client shall keep all usernames, passwords, IP addresses, and computer names strictly confidential, and is solely responsible for any liability or damages resulting from its or an Authorized User's failure to maintain confidentiality of such information.

d. Client is solely liable for all activities on the Workspace or originating from Authorized Users' IP addresses, including those non-compliant with the Documentation and/or any written instruction. If Client believes unauthorized activity has taken place on the Workspace or in relation with the Workspace, Client must immediately notify DataDome.

e. Except as expressly provided above in the present Section, Client shall not, and shall use reasonable efforts to ensure that other parties under its control do not:

   i. use the Workspace for any use other than for its own purposes;

   ii. provide access to the Workspace to any person other than Authorized Users;

   iii. reproduce or distribute, in whole or in part, the Services;

iv. modify, translate, reverse engineer, decompile, disassemble the Workspace, or otherwise attempt to defeat, avoid, bypass, remove, deactivate or otherwise circumvent any Workspace protection mechanisms or components thereof, including any such mechanism used to restrict or control the functionality, or to derive the source code or the underlying ideas, algorithms, structure or organization from the Workspace or any components thereof;

v. alter, adapt, modify or translate the Workspace in any way for any purpose, including error correction;

vi. distribute, rent, loan, lease, transfer, use in a service bureau or grant any rights in the Workspace or modifications thereof in any form to any person except to the extent expressly permitted under this Contract or with the prior written consent of DataDome;

vii. file any patent or other applications for intellectual property protection with respect to the Workspace, or any information contained in either of the foregoing;

viii. set up a service in competition with the Workspace or DataDome's activities; or

ix. use the Workspace in violation of applicable laws.

3.2 Auditing and Reporting

DataDome may, from time to time, at its own discretion, audit Client's usage of the Workspace, including the number of activated endpoints and Authorized Users. Upon DataDome's request, Client agrees to provide all information reasonably necessary for DataDome to audit its use of the Services and its compliance with this Agreement.

3.3 Evolution

Client agrees that DataDome may, at its own discretion, develop and/or evolve the Services, including by adding or adjusting functionalities without negatively impacting the Client's use of the Services.

3.4 Prerequisites

DataDome provides a list of the technical prerequisites in the Documentation, which Client must comply with before accessing the Workspace.

(i) Client understands that the Services are provided based on the specific criteria and rules set out by Client. Client is solely liable for configurating such criteria and rules in Workspace, according to their needs and constraints. DataDome does not provide customised configuration services.

(ii) Client shall maintain their internal systems, equipment, and technical environments, to the standards described in the Documentation. DataDome's requirements are listed on: https://docs.datadome.co/docs.

DataDome shall not be liable if Client cannot use the Workspace due to lack of compliance with the prerequisites or other unambiguous, written instruction provided by DataDome to Client.

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

3.5 Cooperation

The Client undertakes to cooperate fully and in good faith with DataDome and to keep DataDome immediately informed of all difficulties and/or information likely to have an impact on the performance of the Workspace.

Client shall designate a person who will be the primary point of contact for DataDome within Appendix 4.

4. CLIENT DATA

4.1 The Client alone is responsible of the accuracy, quality, integrity, reliability, suitability and intellectual property rights of and in all Client Data. Neither DataDome nor its suppliers will be responsible for Client's elimination, correction, destruction, damage, loss or error arising during the storage of the Client Data by DataDome or its suppliers.

4.2 Client represents that Client's Data, the processing of the Client's Data and any other activities in connection with the Services do not violate, infringe or misappropriate any third party's rights.

4.3 Any Client Data may be deleted and/or discarded by DataDome if the Client breaches this Agreement, including without limitation the obligation to pay any Fees set out in an Order or an additional invoice.

4.4 For purposes of maintenance, statistics and for developing, improving and providing DataDome's products and services, Client Data may be randomly and anonymously recorded and processed by DataDome and its technology suppliers.

5. DATADOME'S OBLIGATIONS

5.1. General Obligation

DataDome shall provide the Services in compliance with this Agreement. The Services do not include customization of the Workspace or setting up the parameters of the Workspace.

5.2. Security

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

For 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 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 take all measures to avoid any misuse or fraudulent use of systems and computer files, including data circulating through the Workspace, by third parties; and
- to take all security measures, including hardware, to ensure the conservation and integrity of data, documents, and processed information.

5.3. Reversibility

At the latest thirty (30) days after the date of effective termination or end of this Agreement, for any reason, DataDome will, at the Client's written request, provide the Client's configuration data on the Workspace in a standard format such as csv or json.
DataDome can also, subject to a specific Order and payment, provide support for migration to another system which can be done directly with a third-party company chosen by the Client.

5.4. Outsourcing

DataDome may outsource a part of the Services to third-party suppliers under DataDome's, without exonerating DataDome of its liability towards the Client for the subcontracted Services.

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

6. FINANCIAL CONDITIONS

6.1. Fees

6.1.1. General

Client shall pay all fees set out in each Order, including the fees for: (i) the Subscription ("**Subscription Fees**"), (ii) the set-up of each Workspace ("**Set-up Fees**") and (iii) each Additional Request used by Client ("**Additional Requests Fees**") (collectively, the "**Fees**"). Client acknowledges that the Set-up Fees are due for each Workspace. For the avoidance of doubt, adding any Workspace during a Subscription Period requires the Parties to enter into an additional, separate Order.

6.1.2. Additional Requests Fees

Each month, Client will receive a status report of the consumption of Requests over the previous month. If the consumption of Requests over the previous month is found to be greater than the subscribed Plan, the Client will pay a monthly supplementary invoice for the Additional Requests as set forth in the Order.

Client is liable for the payment of all Additional Request Fees, even if it is due to an Affiliate's consumption.

6.2. Payment Terms

Client will pay the Fees on the payment terms set forth in the Order.

6.3. Payment Delay

In the event of a payment delay of more than fifteen (15) days, access to the Workspace may be momentarily interrupted, without notice. In such an event, access to the Workspace shall be restored as soon as the payment from the Client has been received by DataDome. 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 the ability of the Client to access the Workspace. Processing of Requests sent from Domain registered within the Workspace shall continue on an on-going basis until termination or expiry of the Contract is effective. Therefore, invoices will continue to be issued for any Requests and Subscription regardless of potential escalation or dispute that may arise.

DataDome will not be liable of any damages resulting from the suspension of Services.

7. DURATION

7.1 Duration of the Agreement

This Agreement enters into force as of the Effective Date, and expires:

(i) If one of the termination events provided in the Termination section occurs, or
(ii) Six (6) months after expiry of the last Order in force.

7.2 Subscription Period (duration of an Order)

The Subscription Period will automatically renew for one (1) year periods. The Client has the option to terminate its Subscription Plan by sending a registered letter with acknowledgment of receipt or via email (with acknowledgment of receipt) at least three (3) months prior to the expiration of the relevant Subscription Period. Termination will then take effect at the end of the relevant 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 a updated price list.

If Client wishes to terminate the Subscription prior to the end of the Subscription Period, no Fees already paid will be reimbursed and all outstanding Fees including for the remaining term of the Subscription Period will be due and payable.

8. TERMINATION

8.1 Termination for breach

In the event of a material breach by either Party of any of its representations, warranties or obligations under this Agreement, the non-breaching Party shall provide notice of the breach by sending a registered letter or email with acknowledgment of receipt to the breaching Party. The breaching Party shall remedy the breach within thirty (30) calendar days (the "**Remedial Period**"). On expiration of the Remedial Period, or if remediation is not possible, the non-breaching Party may request termination of the Agreement, including the applicable Order, which will take effect on receipt of the written, termination notice by the breaching Party – such notice to be sent in a 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 Agreement **or** (iii) failure to comply with applicable laws pertaining to collection or processing of Personal Data, the non-breaching Party will be entitled to terminate this Agreement and the applicable Order effective upon delivery of written notice. The termination notice will be sent in a 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.

8.2 Effects of any termination

At the end of the Subscription Period or where the Agreement is terminated early (other than a termination by Client for an uncured breach by DataDome), Client shall pay any outstanding invoices, in accordance with payment terms provided in the Order, including invoices through the expiry of the running Subscription Period.

At the effective date of termination or expiry of the Agreement, access to the Workspace will be removed and Client Data will be deleted by DataDome, in compliance with Article "Reversibility", without liability.

9. 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 business or respective activities as well as to the Agreement, and that this information may be delivered in writing, verbally, or by any other means ("Confidential Information") in connection with this Agreement.

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 Workspace, 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 this Agreement:

(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 to exercise its rights or perform its obligations under this Agreement, 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 this Agreement, and
(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.

The obligations referred to in paragraphs (i) to (iv) above shall not apply to Confidential Information 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 lawfully known by the receiving Party, 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 receiving 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 lawfully obtained by the receiving Party via a third party, who in disclosing, breaks no confidentiality obligation,

- is developed independently by the receiving Party without use of the Confidential Information, or
- is disclosed by the receiving Party with prior written agreement of the disclosing Party.

The confidentiality obligations shall apply for the duration of this Agreement as well as for a period of five (5) years after expiration or termination of this Agreement for whatever reason.

10. INTELLECTUAL PROPERTY

DataDome and its licensors hold all rights, title, and interest, including all intellectual property rights, in the Services, the Workspace, and DataDome technology, software, content, applications, user interface, and all development work carried out for Client in connection with this Agreement, including copyrights, trademarks and logos. All rights not expressly granted to Client in this Agreement remain reserved by DataDome and its licensors. Client's right to access the Service does not confer upon Client any property right to or in the Service. Client is not allowed to remove any trademarks, logos, copyright notices or any other intellectual property notices, used by DataDome to identify its products. The license provided herein is not a sale.

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.

11. INFRINGEMENT WARRANTY AND INDEMNIFICATION

DataDome will defend and indemnify the Client, at its sole expense, against any third-party action or suit against the Client alleging that the Workspace, when used by Client and its Authorized Users in accordance with this Agreement, infringes such third party's intellectual property rights (a "Claim") 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 defense 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's obligations detailed above shall not apply to an infringement claim to the extent resulting from modifications or combinations of the Workspace by the Client or third parties acting on its behalf, that were not expressly authorized in writing by DataDome.

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

12. PERSONAL DATA

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

13. 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.

14. LIMITED REPRESENTATIONS AND WARRANTIES

Each Party represents and warrants to the other Party that it has full authority to enter into this Agreement.

Client represents and warrants to DataDome that the Client Data and the processing of the Client Data by DataDome and its subprocessors do not and will not violate applicable law or infringe or misappropriate any third party's intellectual property rights or any other rights of any third party.

DataDome warrants to Client that it will provide the Services and the Workspace in compliance with this Agreement. This warranty does not cover: (a) parts of the Service or the Workspace that have been subject to misuse, tampering, experimentation, alteration, or negligence by Client or any third party on behalf of Client; (b) issues arising from Client's network connections or caused by the Internet; (c) damages that occur due to a Force Majeure Event; (d) any other materials or services provided by anyone other than DataDome; and (e) repairs to the Workspace or Service by anyone other than DataDome.

Except as expressly provided in this Agreement, the Services and the Workspace are provided "as is", and DataDome does not make any other warranties or representations of any kind, express, implied or statutory, including relating to their availability, reliability, accuracy, merchantability or fitness for a particular purpose. The Services may include certain Open-Source Software, governed solely by the applicable open-source licensing terms, and will be provided "as is". DataDome provides no warranty specifically related to any Open-Source Software or any applicable Open-Source Software licensing terms.

15. LIABILITY

The Parties are only liable for direct damages caused to the other Party resulting from the performance of the Contract. Neither Party is liable to the other Party for any indirect, consequential, or incidental damages, including loss of data or use of data or lost profits.

Except with respect to each Party's gross negligence or willful misconduct and Client's obligation to pay Fees, each Party's maximum aggregate liability to the other Party in connection with this Agreement will not exceed the amount invoiced to the Client for the Services in the last twelve-month period immediately preceding the occurrence of the event giving raise to the damage.

To the extent not prohibited by applicable law, any claims for legal action under this Agreement must be brought by one Party against the other Party within two (2) years from the date when the right to take such legal action arose or accrued. This period can be further limited if the statute of limitation is shorter.

16. 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.

17. JURISDICTION

This Agreement will be governed by and construed in accordance with the laws of the State of New York excluding its conflict of laws rules. Each of the Parties irrevocably agrees that the courts located in the City of New York, Borough of Manhattan, New York, will have exclusive jurisdiction to hear and determine any action brought under this Agreement, and each Party irrevocably submits to the jurisdiction of such courts. The Parties agree that the United Nations Convention on Contracts for the International Sale of Goods will not apply to this Agreement.

18. MISCELLANEOUS

18.1. Entire Agreement; Amendments.

The Agreement covers the final and exclusive agreement of the Parties regarding the subject matter of this Agreement. Previous agreements reached between the Parties regarding the subject matter of this Agreement are superseded by this Agreement. In the event of any conflict between this Agreement (excluding the appendices and the Terms of Use), any Order, the Terms of Use, and any of the appendices, the following order of precedence applies: (a) DataDome's data processing agreement, (b) the Order, (c) the other appendices to this Agreement, (d) this Agreement (excluding the appendices), and (e) the Terms of Use.

Any amendment to this Agreement must be made by written, mutual agreement between the Parties.

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

18.2. 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 Agreement, covering DataDome's liability to Client under this Agreement.

18.3. Notices

Unless otherwise provided in this Agreement, email notices delivered by either Party under this Agreement shall be deemed to have been validly served on confirmation of receipt of the email.

Where the terms of this Agreement require a notice to be sent with a registered letter, it shall be deemed to have been served on the date of first delivery attempt by postal services or nationally recognized courier. All registered letters must also be sent by email.

18.4. 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 Agreement.

18.5. No Partnership

The Parties declare that this Agreement 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 this Agreement shall constitute one Party as an employee, agent, joint venture partner or servant of the other Party

18.6. Severability

If one or more of the provisions contained in this Agreement shall be held to be invalid, illegal or unenforceable, in any respect, the validity, legality and enforceability of the remaining provision contained herein shall not in any way be affected or impaired, but the Agreement shall be construed as if such provision were not a part of this Agreement. The Parties shall meet promptly to discuss alternative provisions to replace any provision that is invalid, illegal or unenforceable. 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.

18.7. Non-Waiver

No waiver of any provision in this Agreement will constitute a waiver of any other provision, whether or not similar, nor will any waiver constitute a continuing waiver. No waiver will be binding unless executed in writing by the party making the waiver.

18.8. Survival

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

18.9. Transfer

Client shall not assign its rights or delegate its obligations under this Agreement to any third-party, without prior written authorization from DataDome.

Either Party may assign this Agreement to a third-party in connection with a sale of all or substantially all of its assets or any 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 transaction.

18.10. Electronic Signature

The Parties agree that this Agreement may be executed and delivered by electronic signatures and that the signatures appearing on this Agreement are the same as handwritten signatures for the purposes of validity, enforceability and admissibility.

The Parties agree that this electronically signed Agreement constitutes literal proof under the meaning of Article 1365 of the Civil Code and has the same probative value as a written document on paper medium in accordance with Article 1366 of the Civil Code. As a consequence, this Agreement signed electronically shall be considered as a literal proof, including in judicial court, of the identity of the signatories and of their willingness to sign its content in the same manner, under the same conditions and with the same probative value as any document drawn up, received, signed and archived on paper medium.

Each Party undertakes to keep the original of this Agreement by its own means and not to compromise its seal, which guarantees its integrity.

19. SIGNATURE

By signing an Order, Client is deemed to be bound by this Agreement.

Appendix 1 – Datadome Data Protection Agreement

Regulation (EU) 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:

1- DEFINITIONS

The terms with a capital letter below shall have the same meaning as in the Regulation or in the Contract.

"**Data Controller**" refers to "the Client" or "You" (depending on the term used in the Contract).

"**Data Processor**" refers to DataDome.

2- DESCRIPTION OF THE PROCESSING

The Data Processor is authorized to process on behalf of the Data Controller the Personal Data necessary to provide the Service(s), and listed in Exhibit A.

3- DATA PROCESSOR'S OBLIGATIONS

3.1 The Data Processor agrees to process the data only in accordance with the Data Controller's documented instructions appearing in Exhibit A and/or in the Contract, and/or any written instruction provided by the Data Controller to the Data Processor during the term of 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 shall 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.

3.2 In the event of a transfer of Personal Data to a country that is not a Member State of the European Union nor a third party country benefiting from an adequacy decision of the EU Commission, or to an international organization, the Parties shall sign the Standard Contractual Clauses published by the European Commission (updated 2021 version):

- when the Data Processor is the exporter and the Data Controller is the importer :
  - Module 4 is applicable;
  - Clause 7 (docking clause) is included;
  - The optional paragraph in Clause 11 is not included;
  - Clause 17 : the Governing law is the one of the Contract;
  - Clause 18 : The competent courts are the ones of the Contract;
  - The SCCs Appendix I (Sections A and B) is completed by the Parties and attached to this Data Protection Agreement.
- when the Data Controller is the exporter and the Data Processor is the importer :
  - Module 2 is applicable;
  - Clause 7 (docking clause) is included;
  - Clause 9(a) : Option 2 is applied;
  - The optional paragraph in Clause 11 is not included;
  - Clause 17 : Option 1 is applied : the Governing law is the one of the Contract or, if the law of the Contract is not the law of an EU Member State, French law;

- Clause 18(b) : The competent courts are the ones of the Contract or, if the courts of the Contracts are not in the EU, the French courts.
- The SCCs Appendices I, II and III (all sections) are completed by the Parties and attached to this Data Protection Agreement.

3.3 The Data Processor agrees to ensure that persons authorized to process Personal Data under this Data Protection Agreement:

- agree to respect confidentiality or are subject to an appropriate legal obligation of confidentiality.
- receive the necessary training regarding the protection of Personal Data.

3.4 Sub Processors

Data Processor shall not provide access to the Personal Data of Data Controller to any third party, with the exception of the subprocessors mentioned in Exhibit A.

Any addition or replacement of the Sub processors shall be notified to Data Controller with a 30-day prior notice.

This notice must clearly indicate the outsourced processing activities as well as the Sub Processor's identity and contact information, 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 fifteen (15) days from the date of the receipt of this information to raise written objections.

If the Parties do not agree on a solution following objections raised by the Data Controller, the Data Processor will be granted the right to terminate the Contract without penalty.

The Sub 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 Sub Processor - imposing on the Sub Processor equivalent obligations on the protection of Personal Data as outlined in the Contract and the Data Protection Agreement.

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

3.5 Data subjects' right to information

Given the nature of the Services, it is the responsibility of the Data Controller to provide information on the Personal Data Processing to the Data Subjects.

3.6 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 Regulation.

When Data Subjects exercise their rights with the Data Processor, the Data Processor shall transfer these requests by Data Controller via any reasonable means. The Data Processor can respond directly to the Data Subject's request only at the Data Controller's instruction.

3.7 Notification of Personal Data breaches

The Data Processor notifies the Data Controller of all Personal Data breaches as soon as possible and, in any case, within seventy-two (72) 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, including :

(i) A description of the nature of the Personal Data breach including, if possible, the categories and the approximate number of Data Subjects 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 Processor 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.

The Data Processor agrees to actively collaborate with the Data Controller in order 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 Data Processor therefore refrains from making such notification and communication.

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

Data Processor shall assist Data Controller in ensuring compliance with its obligations pursuant to Articles 32 to 36 of the Regulation taking into account the nature of processing and the information available to the Data Processor.

Data Processor shall make available to Data Controller all information necessary to demonstrate compliance with Data Processor's obligations laid down in Article 28 of the Regulation and allow for and contribute to audits, including inspections, conducted by Data Controller or another auditor mandated by Data Controller pursuant to Article 5.

3.9 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.

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 Exhibit A. The Data Processor agrees to maintain these measures throughout the entire Contract period.

3.10 Fate of the data

Upon termination of the Contract the Data Processor agrees, at Data Controller's choice:

- 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, or to send the Personal Data to another data processor designated by the Data Controller and then,

and

- to destroy all Personal Data and manual or computerized files containing the information collected within a timeframe of two (2) months after its return, 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.

ARTICLE 5 - DATA CONTROLLER'S OBLIGATIONS

The Data Controller agrees:

- to provide the Data Processor with the Personal Data listed in Exhibit A;
- 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.
- Not to give to the Data Processor instructions which do not comply with the Regulation.

6 - COOPERATION IN THE EVENT OF AUDIT

Data Processor shall keep records in a reasonable manner evidencing that it complies with its obligations pursuant to this DPA and will allow Data Controller to audit such evidence to verify its compliance, with a sixty (60) days prior written notice.

Such audit may be conducted by either Data Controller’s own staff or by a third-party auditor under contract with Data Controller, provided such third-party auditor is subject to a non-disclosure agreement. All audits must be conducted remotely and shall be limited to five (5) business days.

The scope of any audits shall be mutually agreed in advance between the Parties acting reasonably and in good faith. Such right shall not be exercised more than once a year.

EXHIBIT A - CHARACTERISTICS OF 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 (purpose of the processing):

- provision of the Services;
- hosting and related production services: DataDome hosts the infrastructures necessary for the Services' functioning.
- DataDome also provides monitoring, technical and application administration and operation of the Workspace.

The nature of operations performed on the data is as follows: collection, generation, analysis, reading and processing, transfer to Client, display, storage, backup, deletion.

Feature	**Bot protection**	**AD Fraud**
Types of Personal Data processed	- user's IP address; - DataDome cookie session identifier (user unique ID); - visited URLs; - country.	- user's IP address; - DataDome cookie session identifier (user unique ID); - visited URLs; - country.
Data Subject categories	Visitors to Client's website/app.	Visitors to Client's website/app that arrive as traffic through interactions with online advertising campaigns.
Processing duration	30 rolling days (with automatic management of deletion beyond 30 days). This duration may be reduced by Client.	30 rolling days (with automatic management of deletion beyond 30 days). This duration may be reduced by Client.

2. Authorized Subsequent Processors

Provider	Mandatory / Optional	Service	Location of data*	Clients concerned
Amazon Web Services	Mandatory	Processing (dashboard & some API servers hosted by them) / Storage (back-ups, SQL)	Depends on the region	All clients
Google Cloud	Mandatory	Processing (API servers) & storage (database back-up)	Depends on the region	All clients
OVH	Mandatory	data pipelines, streaming analytics, CDN hosting	Depends on the region	All clients
Scaleway	Mandatory	Processing - only EU - (API servers) Storage - worldwide - (elasticsearch) Data pipelines & streaming analytics - worldwide.	Depends on the region	All clients (EU clients: processing and storage and analytics Other clients : storage and analytics only)
Auth0	Mandatory	Processing (user authentication management) / Storage (list of logins and passwords)	EU	All clients
Vultr	Mandatory	Processing (API server)	USA	US clients only VULTR’s server might be used in the USA (but it could also be GCP or AWS) depending on the location of the user and/or the customer.

**Localisation depends on the region* means : it depends on the country the Data Controller is located. Ex: if the controller is located in the EU it is the EU. If the controller is located in the USA it is the USA.

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

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, the infrastructures on which the DataDome software solution is hosted are located in France.
- The DataDome Modules, installed on clients’ web servers, create a connection with our Account Fraud Protection 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, MFA is available and can be enforced for all users. Moreover customers can enforce IP restriction to access to the Dashboard.

- DataDome uses encryption in transit: All communication across the Internet between users and the DataDome processing system are secured and encrypted using transport TLS 1.2 (or stronger) protocol. The communications between the internal components of the Account Fraud Protection solution are encrypted with TLS 1.2 (or stronger) protocol.
- DataDome uses encryption at rest: Databases managed by Amazon RDS are encrypted using AES-256 provided by AWS Key Management Service (AWS KMS).
  Customer data is stored in Elasticsearch, all the cluster node disks are encrypted at rest using AES-256.
  Moreover, DataDome applies an extra layer of application encryption for User ID fields stored onto the Elasticsearch index thanks to AES-256. The encryption key is stored in a dedicated vault. Data is encrypted at rest and they are only unencrypted when the information is requested from DataDome’s Dashboard and to improve the DataDome detection techniques against bots and fraudulent actors.
- An Audit Trails feature is available from the Dashboard to monitor all the activity on the DataDome customer account.
- Industry-standards technical and organizational security measures such as : Ensuring Data availability; Encryption in transit and at rest; Integrating privacy protection in projects; Logical access control; Managing personal data violations; Monitoring and Supervision; Third-party risk assessment; Managing Relations with subprocessors; Network and system hardening security; Vulnerability management and response plan; Patch management; Security incident response procedure; Traceability (logging); Physical access control; Backups; Minimising the amount of personal data processed; Security Awareness Training; Change management with SDLC procedure.

Appendix 2 – 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:

$$A = (MMA – DT) x 100/MMA$$

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 Order.

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 analyse/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.	On call 24/7 onduty@DataDome.co Monday-Friday 9:00 am - 7:00 pm CET & EST	2 h	8h (4h)

	- DataDome is completely unavailable or inaccessible to its Clients	support@DataDome.co		
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.

Appendix 3 – Business model and feature list per Plan

The Subscription to the DataDome services is a function of the number of monthly Requests processed by the DataDome servers.

1. Set-Up

A set-up is charged for each addition of a new Workspace to the Subscription in accordance with the rate conditions specified in the Order.

2. Rate Grid

The basic flat rate subscription covers the processing of Requests up to the maximum monthly consumption of Requests subscribed by the Client.

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 monthly invoice.

The price of the basic Subscription and the price of the additional billing depend on the type of subscribed offer, yearly billing offer or monthly billing offer. It is specified in the Order.

The over consumption is calculated at the Subscription-level. If the Client benefits from multiple Workspaces, the total consumption is equal to the addition of the total number of requests processed through each Workspace.

3. Features

All features by Subscription plan are available at the following link: Features.