USER AGREEMENT

1. The following document regulates the rights and obligations of the users in connection with the user's usage of the services provided by **BlockchainAds Labs LLC** with a registered office in Suite 305, Griffith Corporate Centre, Beachmont, Kingstown, St. Vincent and the Grenadines.
2. This document applies to entities (including natural persons) that use the services of the Operator, including Blockchain-Ads network, as well as visitors to the websites of the Operator.
3. The following terms shall mean:
    1. Agreement - concluded between the Operator and the User, the content of which shall be specified in these Regulations. The Agreement is concluded by acceptance of the Regulations.
    2. Fee - the charge paid to carry out the commissioned advertising campaign.
    3. Operator - Cipher S.A with registered office in Avenida Amilcar Cabral 889, Cidade de S. Tomme at St. Vincent and the Grenadines (ST), operating the website and providing the Services in accordance with the Regulations.
    4. Regulations - this document determining the rules of using the services of the Operator.
    5. Services - services provided in electric means, indicated in the Regulations.
    6. User - each person or entity that uses Services under the Regulations, including registration.
4. The Operator reserves the right to choose whether to accept the User to use its Services.
5. In the case of natural persons, the services may only be used by persons who are at least 18 years old and have full legal capacity.
6. The Operator may request access to the Analytics account in order to verify the quality and authenticity of the traffic if the Operator has reason to believe that the data is false.
7. Each person or entity is required to read the Regulations and policies before using the Services.
8. Agreement shall govern participation in the Operator program.
9. By using the Operator website and/or platform, the User agrees to these Regulations.
10. A person acting on behalf of another entity shall have the appropriate authorisation of the represented entity.

11. The Services are provided for the duration specified in the offer selected by the User. The offer specifies the time and manner of running the campaign, related costs, method of payment.
12. The entity with the status of a consumer acknowledges and agrees that the provision of services will start before the deadline for withdrawal from the Agreement. This may be due to the necessity to perform the Service in accordance with the offer.
13. The Operator provides the following Services:
    1. access to the content of the operator's website;
    2. account access for registered Users;
    3. data collection and provision of data on advertising campaigns and their effects, measurement and analysis in the dashboard.
14. The following provisions apply to the provision of advertising services.
15. Operator will not accept any advertisement that can harm or that is inappropriate for the general audience.
16. The following advertisement types are examples of prohibited advertisements:
    1. advertised page(s) that contain any popup/popunder or page blocker;
    2. advertised page(s) that contain any kind of content prohibited in the websites section;
    3. advertised page(s) that contain scripts that alter the user’s browser settings;
    4. advertised page(s) that contain any frame-breaking codes;
    5. advertised page(s) that contain multiple alert boxes;
    6. advertised page(s) that contain alert boxes with "Close" buttons that cannot be seen by users.
17. Each advertising campaign is subject to approval by the Operator.
18. If, after approval, the advertising violates the Terms of Use, the campaign and account will be blocked.
19. If changes are made to the website, services, content covered by an advertising campaign, the Operator must be notified immediately. In such a case, the Operator shall not be held liable if the changes have been made of which he has not been informed within a reasonable time before the changes were made. The Operator shall not be liable if it is not possible to adapt the Services to the changes.
20. Notification of changes should be made by e-mail or through the notification system.
21. If any kind of malware is detected, e.g. exploits, hijackers or viruses, the account will be disabled and the User will not be entitled to a refund. The above rules shall also apply in the situation of detecting activity by entities whose accounts have been blocked.
22. There is no entitlement to reimbursement of the Fee in the situations described above.
23. Campaign-related information and materials will be subject to removal if:
    1. they relate to a project that has been proven to be a fraud;

    2. the project is no longer active;
    3. the type of activity has been changed and the content does not reflect the current actual activity.
24. If any of the aforementioned conditions are met and the content will be deleted. Operator is in no way responsible and a refund will not be possible.
25. If the publisher deletes campaign-related information and materials delivered to his website through the Operator service, the publisher is required to notify Operator in regards to the deletion as well as the reason behind the decision.
26. If the publisher does not provide a valid reason for deleting the article, he will be required to fully refund the cost of the said article to Operator. Valid reasons for article deletion include:
    1. the project was proven to be a scam;
    2. the project is no longer active;
    3. the domain of activity has been changed and the content is no longer reflecting the current activity of the advertiser.
27. If the publisher does not refund the cost of the article he deleted, its account will be locked.
28. All campaigns on Operator are served, tracked, and reported by Operator. For campaigns that involve third-party serving/tracking, accounting may be beyond Operator's control.
29. The data generated by the campaign will only be available for 1 year, but no longer for the duration of the Agreement.
30. After this time, this data will be automatically deleted from the user's account. The user is solely responsible for downloading and saving this data if the user wishes to do so.
31. Before starting an advertising campaign, the required Fee must be paid according to the offer of the Operator.
32. Information on how to pay the Fee is provided via account.
33. In order to use selected services (such as advertising), the User must register and send an email.
34. In order to receive a bill or an invoice, all the necessary customer data must be provided.
35. The Operator may contact the User in order to complete the profile. If the User refuses to provide the necessary details, the campaign order shall be rejected.
36. The invoice and the payment document will be forwarded to the recipient electronically, at the e-mail address indicated.
37. Services will commence as soon as payment is received and accounted for.
38. Payments and settlements shall be made from the funds held in the deposit of the relevant User.
39. The Operator accepts deposits in the following cryptocurrencies: xADS
40. The User may only fund the deposit with cryptocurrencies accepted by the Operator.
41. If you wish to make deposits in other cryptocurrencies, please contact the Operator first or use an external provider.

42. All Fees are subject to change at any time. It is recommended that you always check the Fee before placing an order.
43. After the service has been requested, a Fee will be charged in accordance with the price list. The Fee will be charged from the funds accumulated within the deposit. In case of insufficient funds, the Operator shall not start the ordered service.
44. Funds held on deposit may be withdrawn at any time.
45. Information on how to create a deposit and the address of the wallet is provided by the Operator.
46. All bonuses granted may be used to purchase Services. Bonuses are not exchangeable for other funds. Unless otherwise stated, unused bonuses will be canceled.
47. The Operator may allow deposits in the form of cryptocurrencies. The Operator does not accept deposits in the form of currencies.
48. The User hereby indemnifies the Operator and the publishers (including their successors, directors, officers, employees, agents, assigns) against any liability as well as claims for advertising campaigns to the extent provided for in the Regulations, as well as in the event that the design, content proves to be unreliable, misleading or unlawful.
49. In cases where the law does not impose liability on the Operator, the Operator shall not be liable for any damages, including those resulting from loss of data, loss of use or loss of profit, or from the provision of services.
50. The Operator is not responsible in the event of loss of account access data by the User or their disclosure to other persons, as well as in the event of system failure or other technological failures, delay in delivery and / or failure to deliver the campaign, including, without limitation, difficulties with the publisher or the website. website, difficulties with a third party server or electronic failure, errors in content or omissions in the URL.
51. Complaints may be submitted in writing to the Operator's address; electronically, via the address contact@blockchain-ads.com
52. The complaint is examined within 14 days from the date of its receipt.
53. The complaint should contain the following information: identification data of the claimant (e-mail address provided during account registration), description of the reported problem, indication of the date of the problem (day, month, year).
54. If the complaint does not contain the information necessary for its consideration, the Operator will ask the person submitting the complaint to supplement it to the extent necessary, and the 14-day period then runs from the date of delivery of the completed complaint.
55. The response to the complaint is sent only to the e-mail address assigned to the User's account.
56. In the event of an appeal against a decision issued on the complaint, the above provisions shall apply accordingly.
57. The law applicable to the Agreement and disputes arising from the Agreement is St. Vincent and the Grenadines law.

58. Any disputes related to the Services provided to entities with the status of consumers will be settled by the competent St. Vincent and the Grenadines common courts.
59. An entity with the status of a consumer has the option of using an out-of-court complaint and redress procedure before the Permanent Consumer Arbitration Court at the Provincial Inspector of Trade Inspection in Poznań.
60. Information on how to access the above-mentioned The mode and procedures for resolving disputes can be found at the following address: https://gdpr-info.eu/, in the "Settlement of consumer disputes" tab. A user who is a consumer may also use the EU ODR internet platform, available at the following internet address: https://gdpr-info.eu/chapter-3/. Detailed information on the application procedure can be found here. The operator may attempt to settle the dispute amicably with the User running a business through an independent mediator, after prior consent to mediation.
61. If the User requests a mediation proposal and the Operator accepts this proposal, the mediation will be conducted by a mediator or mediators from the Wielkopolska Center for Arbitration and Mediation at the Wielkopolska Chamber of Commerce and Industry, in accordance with the mediation regulations applied by the Center. The operator will bear a reasonable share of the total mediation costs, which will be agreed by the parties from time to time. The list of mediators and mediation regulations are available at: https://caim.com.pl/.
62. The Operator informs that in connection with the use of electronic services, users remain exposed to threats, min. as:
    1. the operation of spyware;
    2. spoofing for phishing purposes;
    3. computer viruses;
    4. spam.
63. Threats concern not only computers, but also other portable devices, e.g. smartphones, tablets.
64. Spyware is one that can be covertly installed on the user's device, e.g. by accessing a crafted website or running a file sent via e-mail. It can monitor / send to the attacker both the data on the device and the user's actions: mouse movements, text typed from the keyboard, start preview / eavesdropping from the camera and microphone.
65. Phishing is the placing on the Internet of fake websites imitating the original ones and forcing users to log into them, e.g. by sending a specially prepared e-mail message that pretends to be a message from an authentic institution or person. The goal is to intercept access data to the service (login, password).
66. A computer virus is a malicious software that spreads by saving an infected file on a data carrier, e.g. a hard drive, USB flash drive. The purpose of the virus is to steal or delete data, disrupt or take control of the device. Most often, infection with a computer virus occurs after downloading files from an untrusted Internet source or opening an attachment in e-mail.

67. Spam is unsolicited or unnecessary electronic messages that are sent to multiple recipients simultaneously. They often carry computer viruses, spyware, and links to malicious websites.
68. In order to ensure safe use of the Internet, each user should:
    1. Take care of the safety of the device used. In particular, the device should have an antivirus program with an up-to-date virus definition database, an up-to-date and secure version of the web browser and an enabled firewall.
    2. Periodically check whether the operating system and programs installed on the device have the latest updates, because the attacks use errors found in previously installed software versions.
    3. Secure access data to services offered on the Internet - e.g. logins, passwords, PINs, electronic certificates, etc. such data should not be disclosed or stored on the device in a form that allows easy access and reading.
    4. Be careful when opening attachments or clicking links in messages that you did not expect, e.g. from unknown senders. In case of any doubts, it is worth contacting the sender.
    5. Use anti-phishing filters or other tools that verify that the displayed page is not phishing.
    6. Only download and install files from trusted sources.
    7. Set up a secure and hard-to-break password for accessing the network (Wi-Fi). It is also recommended to use trusted standards for encryption of Wi-Fi wireless networks, such as WPA2.
    8. Control physical access to devices.
69. The Operator pays due attention to the protection of privacy.
70. Using the Services, including registration, requires providing data, including personal data.
71. The data controller of the User's personal data is the Operator.
72. Before using the Services, please read the rules for the processing of personal data available in Privacy Policy.
73. The business user (hereinafter referred to as the "Client") commissioning the Operator to provide advertising services (such as website traffic measurement) shall ensure that the users whose activity is to be monitored and about whom information is to be collected by the Operator in order to provide the commissioned service have given all necessary consents as required by law, as well as that they have been adequately and sufficiently informed about the Operator's activities. The Client shall be liable to the Operator for all damages suffered by the Operator if the Client fails to fulfil its obligations under this agreement, in particular the Client shall reimburse the Operator for the amounts paid by the Operator on account of penalties imposed on it by public authorities and compensation paid.
74. The Operator is entitled to amend the Regulations in the event of:
    1. changes in legal regulations or their interpretation;

2. the imposition of certain obligations by state authorities;
3. changes in fees;
4. organizational changes, including those related to the operation of the Software or User service;
5. technological and functional changes;
6. changes in the scope of the Services or functionalities provided, including the introduction of new ones;
7. editorial changes.

75. The amendment to the Regulations becomes effective within 15 days from the moment of notification of the changes and the availability of the new version of the Regulations.
76. The Operator will inform about the change in the Regulations and the possibility of accepting the change during the first login to the account, from the moment the changes come into force.
77. The new version of the Regulations will be published on the Blockchain-Ads.net website and sent to the e-mail address assigned to the account.
78. The Operator reserves the right to amend the Regulations without observing the 15-day deadline, with immediate effect, in the event of:
    1. when the introduction of changes results from a legal obligation or a decision of the competent authority, and the necessity to introduce the required changes makes it impossible to comply with the above-mentioned 15-day notification period;
    2. the change is necessary due to the need to counter fraud, malware, data breaches or other cybersecurity threats.
79. The changes may be accepted or not. In the absence of express acceptance of the new version of the Regulations, the first action performed after the amendments come into force shall be deemed to consent to the provision of Services under the new rules.
80. In the event of non-acceptance of the changes, in order to terminate the Agreement, the Operator must be notified immediately, not later than within 15 days from the announcement of the changes, via e-mail contact@blockchain-ads.com.
81. Termination of the Agreement in the above-mentioned mode takes effect 15 days after notification of the changes to the Regulations.
82. The User has the right to terminate the Agreement with a 30-day notice period.
83. The Operator has the option to terminate the Agreement with a 30-day notice period in the event of repeated breaches of the Regulations.
84. These Regulations are available in the English version, available at the following internet address: https://github.com/Blockchain-Ads/Blockchain-ads/blob/main/documentation/terms%26conditions.pdf.
85. If any provision of the Regulations is considered invalid by a final court decision, the remaining provisions shall remain in force.
86. The Regulations are valid from 01.01.2022

ADVERTISING POLICY & RULES

1. Since high-quality advertisements help to maintain the standard of the network, but also increase advertisers' conversions, advertising material should be prepared diligently.
2. General rules for advertisers:
    1. Advertising content should comply with the law and the guidelines of the competent authorities. In particular, it is prohibited to advertise illegal products or services.
    2. Advertising content should be consistent with good morals and must not offend or discriminate against any social or ethnic group.
    3. Vulgar content and nudity are prohibited.
    4. Advertisements should be prepared with due care, i.e. meet the aesthetic requirements and not overload the website.
    5. Projects advertised online should work, provide valuable content and not be a scam or other type of scam.
    6. Abuse and deception of our or other advertising networks is prohibited.
    7. Landing pages that are blacklisted or contain any malware (virus, exploit, malware, hijack) may not be advertised on the network.
    8. Content in advertisements should be consistent with the actual product or service advertised. In addition, it is forbidden to advertise reflinks to websites, which in their regulations prohibit such advertising.
3. In case of non-compliance with these rules, the Operator shall not be held responsible and may refuse to provide services or cease to provide them. Money spent on campaigns is not refundable.
4. All advertising formats are subject to review and approval. The Operator reserves the right to reject any campaign without giving any reason.
5. Rules regarding ad formats:
    1. Acceptable ad formats are .jpg, .png, .gif in size max 0.5MB. In the case of .gif extensions, remember to optimize the file so that all transitions are smooth and do not overload the website.
    2. HTML ads packed in .zip extension are acceptable. The packages should contain all elements inside and no externals are allowed.
    3. It is forbidden to place in the advertisement direct links to pages with popup and popunder or banners without permission of the adserver operator.
    4. The use of iframes, popups and popunder is prohibited. These formats are only used in a few specific cases and may be approved with prior approval. Requests should be sent to contact@blockchain-ads.com. Repeated addition of these formats, despite rejection, will result in a ban.
6. Any attempt to manipulate the user, tracking, frame-breaking codes will result in a lifetime ban, which cannot be appealed. This also applies to ads that are blocked by your browser, firewall and antivirus.
7. The user may use the media plan service. All payments for the creation of a media plan should be paid before the service is provided and are non-refundable. Should the User

wish to use their own media plan they should make an appointment with a member of the team by contacting contact@blockchain-ads.com. Pre-payments for the plan should be made before the plan is executed. These are partially refundable if the User cancels part or all of it before the compliance procedure begins and if the publisher decides to reject the material during the compliance procedure, does not take any action on the requested activities and does not issue a payment document for them. The publisher, after publishing the content, may remove it if it turns out that the advertised project is a fraud, is not active or the published content is incorrect and does not reflect reality. The advertiser may demand a refund if the above conditions are not met.

8. Repeatedly adding a campaign that has been rejected may result in your account being permanently banned. Additionally, if a banned user keeps creating new accounts to circumvent the restriction, all their accounts will be banned for life. You may file a complaint in accordance with the User Agreement available at https://github.com/Blockchain-Ads/Blockchain-ads/blob/main/documentation/terms%26conditions.pdf
9. Neither Operator nor the participating parties will be liable in any way for any damages resulting from the use of the software provided, including, but not limited to, advertising campaign errors and their consequences, website and code malfunctions, non-delivery/incomplete campaign delivery and any difficulties in its operation, technical failures and their consequences, delays, lack of access to the advertising system and other unforeseen difficulties.
10. Operator reserves the right to change any point of the terms and conditions and at any time without notice to you, who are required to keep this agreement under constant review.
11. In matters not covered by these Policy, the user agreement shall apply.

WEBSITE ACCEPTANCE POLICY

1. This document describes the rules for acceptance of parties and provision of services by the Operator. The User is obliged to become familiar with the content of the rules described below.
2. The Operator informs that it will only accept websites that are suitable for hosting advertising formats.
3. The Operator may request access to your Analytics account to verify the quality and authenticity of your traffic if it reasonably suspects that the data is fraudulent.
4. All Users who wish to use the Operator's services must comply with the following rules regarding websites and content:
    1. The website, as well as links and content, must not violate laws, guidelines of competent authorities.
    2. Users may not be asked to click on or be directed to any website or activity containing illegal content, illegal activities, harmful content, malware, or websites

operated by entities competing with the Operator or promoting the activities of entities competing with the Operator.
3. Traffic on the website should not be motivated by rewards for the user's presence or any other activity performed by him/her on the website.
4. The site should not be involved in any illegal activity that may harm the welfare of the user or cause any financial loss by promoting suspicious, nefarious, spam or fraudulent projects.
5. The site should not incite visitors to hatred, racism, violence or any activity that may cause moral or physical harm.
6. Banners must be placed in high visibility areas (above the fold). Banners must not be hidden or distorted in any way, shape or form.
7. Banners must be placed individually in the chosen location. Placing other banners together with banners from the Operator is prohibited.
8. A banner must not be displayed on any page other than the one for which it has been approved.
9. It is prohibited to artificially generate traffic, including buying traffic from other sources (advertising networks or other websites), which will then be sent to our advertisers' websites through their banners.
10. Website refreshment is prohibited in order to increase the number of times you see the banners displayed.

5. The Operator reserves the right not to start the service, discontinue the service and delete the website, if the website uses any kind of false, motivated or purchased traffic or unethical methods to generate income. In such a case, the Operator is not liable and the revenue from that account will be removed.
6. The above provision includes but is not limited to: autosurfs, iframes, bots, proxies, auto-hit services, traffic exchange systems.
7. Types of websites that will not be accepted on network:
    1. Sites containing or linking to any form of illegal activities;
    2. Sites with inappropriate or violent content and/or vulgar language;
    3. Sites promoting any type of hate-mongering (i.e. racial, political, ethnic, religious, gender-based, sexuality-based, personal, etc.);
    4. Sites that participate in or transmit spam using any kind of online means;
    5. Sites promoting any type of illegal substance or activity or sites with illegal, false, or deceptive investment advice and money-making opportunities;
    6. Sites that are using free domain names;
    7. Sites that don't have a unique design, that are filled with ads, that have more than 1 popunder and/or ask users to click on ads;
    8. URL Shorteners;
    9. Faucet websites;
    10. Websites with pornographic content;
    11. Websites created with the intention of sending bots/fake traffic to our network;
    12. Websites with no original content;
    13. Websites generated on platforms like Wordpress or Blogspot;
    14. Pay to click websites;

15. Automatic/manual traffic exchanges;
16. Any website that has incentivized traffic;
17. Any website that, after it was reviewed by our team, wasn't deemed suitable for our Publisher program;
18. Websites that represent a coin, ICOs, or projects that raised funds from the community.

8. If a site is rejected, you may report the situation and submit a request for reconsideration.
9. The operator reserves the right to refuse to include any website in the display network, without giving a reason for its actions.
10. The Operator reserves the right to change the website acceptance policy. You are required to comply with any changes to the website acceptance policy within 2 days of the update and are required to read this page periodically.
11. This version is effective as of 27.08.2021 r.

Data Processing Agreement Definitions and Interpretations For the purposes of this Agreement, capitalized terms shall have the following meanings, unless defined elsewhere in the Agreement: "Business Day" shall mean any day except any Saturday, Sunday or a public holiday in the respective countries of incorporation of the Parties to this Agreement; "Competent Data Protection Authority" shall mean the competent data protection authority, which, by way of example, could be the St. Vincent and the Grenadines Data Protection Authority. "Data Protection Legislation" shall mean all applicable data protection legislation, including the GDPR, any national data protection legislation, and any regulations, mandatory guidelines or any other mandatory codes of practice issued by any Competent Data Protection Authority, each as amended from time to time; "GDPR" shall mean Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as amended from time to time; "Main Agreement" shall have the meaning given to it in clause 2.1. of this Agreement; "Personal Data" shall have the meaning given to it in clause 3 of this Agreement. For the purposes of this Agreement, the terms "controller", "processor", "data subject", "process", "processing" and "data breach" shall have the meanings attributed to them in the GDPR. Purpose of this Agreement The Data Controller and the Data Processor are parties to one or more (concluded in parallel or by way of prolongation) agreements relating to the provision of advertising services by the Data Processor to the Data Controller (the "Main Agreement"). The purpose of this Agreement is to determine the roles and responsibilities of each Party during the provision of the services under the Main Agreement in order to ensure the Parties' compliance with the applicable Data Protection Legislation. Personal Data, Data Subjects, Processing Operations The Data Processor shall process on behalf of the Data Controller the following types of personal data of the following categories of data subjects: IP addresses of end users of the Data Controller Geographical coordinates (if applicable) of end users of the Data Controller information on terminal devices information on visited services (the "Personal Data"). The Data Processor shall process the Personal Data on behalf of the Data Controller for the purpose of the provision of the services under the Main Agreement. The Data Processor may not process Personal Data in a way that is incompatible with the purpose under this Agreement in relation to the Main Agreement as set out above. Term and Termination This

Agreement shall commence on the date it is signed and shall continue in full force and effect until the expiry or termination for any reason of the Main Agreement on which date this Agreement shall automatically terminate without liability. Upon termination of the Agreement the Data Processor shall proceed in accordance with clause 5.15 of this Agreement. Obligations of the Data Processor The Data Processor shall process Personal Data only for the purpose of the Main Agreement. The Data Processor may not process Personal Data for its own purposes. The Data Processor shall process Personal Data in accordance with the instructions of the Data Controller and in compliance with the Data Protection Legislation. The Data Processor shall immediately inform the Data Controller if the Data Processor believes that any of the instructions of the Data Controller violate the Data Protection Legislation. The Data Processor shall keep a written record of all categories of processing operations carried out on behalf of the Data Controller. This record shall contain: the name and contact details of the Data Processor, of each manager acting on behalf of the Data Processor and, where appropriate, of the representative of the Data Controller or the Data Processor and the data protection officer; the categories of processing operations carried out on behalf of the Data Controller; when applicable, personal data transfers to a third country or international organisation, including the identification of the said third country or international organisation and, in the case of transfers indicated in Article 49, Section 1, paragraph 2 of the GDPR, documentation on appropriate safeguards. The Data Processor shall not disclose Personal Data to third parties, unless (i) to its sub-processors, (ii) with the express prior written consent of the Data Controller or (iii) when legally acceptable. For the avoidance of doubts, the Data Processor´s affiliates and subsidiaries shall not be considered third parties. The Data Processor may disclose Personal Data to other processors working for the Data Controller, pursuant to the Data Controller’s instructions. In this case, the Data Controller shall identify, in writing and in advance, the entity Personal Data shall be disclosed to, the Personal Data to be disclosed, and the security measures to be applied for the disclosure. The Data Processor shall obtain Data Controller's prior consent to transfer Personal Data to an international organization or a third country. The obligation to obtain the consent applies in particular to entrust the processing of Personal Data to Sub-processors. The Data Processor has the right to engage sub-processors on condition that each of them will observe the binding regulations on personal data protection. In case of a planned entrusting the data processing to another sub-processor, the Data Processor shall notify the Data Controller in writing with at least 10 (ten) Business Days in advance, indicating the processing operations to be subcontracted to the sub-processor, and clearly and unambiguously indicating the sub-processor and its contact details. If within 10 (ten) Business Days of receipt of the notification, the Data Controller notifies the Data Processor in writing of any objections on reasonable grounds to the proposed appointment: The Data Processor shall cooperate with the Data Controller in good faith to make available a commercially reasonable change in the provision of the data processing services agreed upon under the Main Agreement; If such a change cannot be made within 90 (ninety) days from the receipt of the notification from the Data Controller by the Data Processor, the Data Controller may, by a written notice provided to the Data Processor, terminate with immediate effect the Main Agreement to the extent that it concerns services which require the use of the proposed sub-processor. The sub-contractor shall be equally obliged to comply with the obligations set out in this Agreement for the Data Processor and the instructions issued by the Data Controller. The Data Processor shall regulate

its contractual relationship with the sub-contractor so that the sub-contractor is subject to the same conditions (instructions, obligations, security measures, etc.) and the same formal requirements for adequate processing of Personal Data and guarantee the rights of the data subjects. The Data Processor shall maintain the duty of secrecy regarding the Personal Data, even after the termination of the Main Agreement. The Data Processor guarantees that the individuals authorized to process Personal Data expressly undertake in writing to respect the confidentiality of the Personal Data and to comply with the relevant security measures, of which they shall be duly informed. The Data Processor shall keep documentation accrediting compliance with this obligation available for the Data Controller. The Data Processor guarantees that the individuals authorized to process Personal Data have the necessary data protection training. The Data Processor shall assist the Data Controller in meeting its obligations in relation to data subjects' requests to exercise rights (i) to access, rectification, erasure and object; (ii) to restriction of processing; (iii) to data portability; (iv) in relation to automated decision making and profiling. The Data Controller shall reimburse the Data Processor for all reasonable costs and expenses incurred with regard to such assistance. When data subjects exercise or declare their wish to exercise their rights under items (i), (ii), (iii) and (iv) above before the Data Processor, the Data Processor shall notify the Data Controller immediately but in any event not later than 72 (seventy-two) hours following the receipt of the request. The notification shall be accompanied by other information (if provided and/or available) that may be relevant to resolve the request. The Data Processor shall notify the Data Controller without undue delay and in any event before the maximum period of 48 hours of any breach it is aware of to the security of the Personal Data it holds, together with all relevant information to document and report the incident. The following minimum information shall be provided, if available: description of the nature of the personal data security breach including, when possible, the categories and approximate number of data subjects affected, and the categories and approximate number of personal data records affected; the name and contact details of the data protection officer or another point of contact to obtain more information; description of the possible consequences of the personal data security breach; description of the measures adopted or proposed to remedy the personal data security breach including, if appropriate, the measures adopted to mitigate possible negative effects. If the above information cannot be provided simultaneously, the information shall be gradually provided without undue delay. The Data Processor shall support the Data Controller in sending prior consultations to Competent Data Protection Authorities, when appropriate. The Data Processor shall support the Data Controller in conducting data protection impact assessments, when appropriate. The Data Processor shall provide the Data Controller with all the information necessary to demonstrate compliance with its obligations under the Data Protection Legislation. The Data Processor shall allow the Data Controller to carry out audits and inspections. The Data Controller is entitled to conduct an audit/inspection at any time, in particular when the obligation to conduct an audit/inspection has been imposed by the supervisory authority or the conduct of an audit/inspection is necessary to explain the identified breach of Data Processor´s obligations under this Agreement. The Data Controller shall notify the Data Processor about the intention to conduct an audit/inspection at least 3 Business Days before the planned start of the audit/inspection. The notification should indicate the exact scope, date and persons authorized by the Data Processor to conduct the audit/inspection. The audit/inspection may be conducted by an independent auditor mutually

agreed by the Parties.. The parties agree on the duration of the audit not longer than 7 working days, unless a longer time is necessary due to the purpose of the audit. In such case, the parties agree on the maximum duration of the audit. The audit ends with a protocol, which contains, in particular, the necessary scope of possible changes in personal data processing. The inspection may be carried out by obliging the Data Processor to answer the questionnaire. The questionnaire may be sent to the e-mail address indicated in clause 7. The Data Processor shall implement appropriate technical and organisational measures to: ensure a level of security appropriate to the risk involved in order to protect the Personal Data from unauthorized use, alteration, access or disclosure, loss, theft, and damage; ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; test, assess and evaluate the effectiveness of technical and organisational measures implemented for ensuring the security of the processing of the Personal Data; pseudonymise and encrypt the Personal Data, as appropriate; prevent a personal data security breach. The minimum technical and organizational measures to be provided by the Data Processor are listed in Attachment No. 2. The Data Processor shall promptly delete all Personal Data provided by the Data Controller in its entirety from its systems and destroy any copies it made of the Personal Data after completing the service, unless and to the extent that the Data Processor is required to retain copies in accordance with the applicable Data Protection Legislation. Obligations of the Data Controller The Data Controller shall provide the Personal Data or otherwise make the Personal Data available to the Data Processor. The Data Controller shall, at the time when Personal Data is obtained, provide the data subjects will all information about the collection and processing of the Personal data and shall obtain any consent (where necessary) of data subjects as required by the GDPR and any other applicable Data Protection Legislation. The Data Controller shall supervise the processing operations performed by the Data Processor. The Data Controller may issue instructions about the type, scope and method of processing of the Personal Data in writing or send to the e-mail address indicated in clause 7 of this Agreement. Contact Point Each Party shall nominate the following contact person within their organisation who can be contacted in respect of queries, complaints or notifications of any kind whatsoever regarding this Agreement or the Data Protection Legislation: Miscellaneous In the event of any conflict between the terms of this Data Processing Agreement and any provision of the Main Agreement and any other agreement between the Parties, this Data Processing Agreement shall take precedence. Notwithstanding the governing law of the Main Agreement, this Data Processing Agreement shall be governed by and construed in accordance with the St. Vincent and the Grenadines law. All disputes, controversy, or claims arising out of or in connection with this Data Processing Agreement shall be subject to the exclusive jurisdiction of the St. Vincent and the Grenadines court(s). The provisions of this Agreement are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision and the rest of this Agreement shall remain in full force and effect. Any amendment to this Agreement must be made in writing upon mutual agreement by the Parties. For the purpose of this Agreement “writing”, “in writing” and “written” includes handwritten signatures, signatures produced by mechanical or digital means (such as scan, digitally scanned and stored signature inserted into [digital] document, etc.) as well as qualified electronic signatures. Also, for the avoidance of

doubt, transmission/exchange in electronic format (for example scanned documents sent by email) do fulfill the form requirement. The written form requirement in this clause may only be waived by respecting the same written form requirement. Attachment No. 1 Minimum technical and organizational measures for personal data security: implementation of a written procedure for personal data protection, which regulates the principles of personal data protection in the processing entity; implementation of a procedure for safe use of IT resources; covering employees or co-workers with trainings in the scope of personal data protection and safe use of IT resources; processing of personal data only after prior written authorization to process the data; covering all persons acting on behalf of the processor with a written obligation to keep secret the information obtained within the framework of providing support services to the Data Controller; processing of the entrusted data in a secure area, covered by access control, physical protection or CCTV video surveillance; use by each employee/co-workers of a separate, unique access account to IT systems in which personal data are processed; applying a policy of strong passwords, forcing a change of passwords and blocking accounts; encrypting mobile devices that process personal data; centrally managed and controlled remote access to personal data; IT systems and software for processing personal data are regularly updated, verified for vulnerability and protected by antivirus systems; protection against unauthorized access to systems and networks through a firewall, as well as using antivirus to preventaccess to malicious websites.

USER AGREEMENT

1. The following document regulates the rights and obligations of the users in connection with the user's usage of the services provided by BlockchainAds Labs LLC with registered office in Suite 305, Griffith Corporate Centre, Beachmont, Kingstown, St. Vincent and the Grenadines).
2. This document applies to entities (including natural persons) that use the services of the Operator, including Blockchain-Ads network, as well as visitors to the websites of the Operator.
3. The following terms shall mean:
    1. Agreement - concluded between the Operator and the User, the content of which shall be specified in these Regulations. The Agreement is concluded by acceptance of the Regulations.
    2. Fee - the charge paid to carry out the commissioned advertising campaign.
    3. Operator -BlockchainAds Labs LLC with registered office in Suite 305, Griffith Corporate Centre, Beachmont, Kingstown, St. Vincent and the Grenadines), operating the website and providing the Services in accordance with the Regulations.

    4. Regulations - this document determining the rules of using the services of the Operator.
    5. Services - services provided in electric means, indicated in the Regulations.
    6. User - each person or entity that uses Services under the Regulations, including registration.
4. The Operator reserves the right to choose whether to accept the User to use its Services.
5. In the case of natural persons, the services may only be used by persons who are at least 18 years old and have full legal capacity.
6. The Operator may request access to the Analytics account in order to verify the quality and authenticity of the traffic if the Operator has reason to believe that the data is false.
7. Each person or entity is required to read the Regulations and policies before using the Services.
8. Agreement shall govern participation in the Operator program.
9. By using the Operator website and/or platform, the User agrees to these Regulations.
10. A person acting on behalf of another entity shall have the appropriate authorisation of the represented entity.
11. The Services are provided for the duration specified in the offer selected by the User. The offer specifies the time and manner of running the campaign, related costs, method of payment.
12. The entity with the status of a consumer acknowledges and agrees that the provision of services will start before the deadline for withdrawal from the Agreement. This may be due to the necessity to perform the Service in accordance with the offer.
13. The Operator provides the following Services:
    1. access to the content of the operator's platform;
    2. account access for registered Users;
    3. data collection and provision of data on advertising campaigns and their effects, measurement and analysis in the dashboard.
14. The following provisions apply to the provision of advertising services.
15. Operator Ad Platform will not process any advertisement that can harm or that is inappropriate for the general audience.
16. The following advertisement types are examples of prohibited advertisements:
    1. advertised page(s) that contain any popup/popunder or page blocker;
    2. advertised page(s) that contain any kind of content prohibited in the websites section;
    3. advertised page(s) that contain scripts that alter the user’s browser settings;
    4. advertised page(s) that contain any frame-breaking codes;
    5. advertised page(s) that contain multiple alert boxes;

6. advertised page(s) that contain alert boxes with "Close" buttons that cannot be seen by users.

17. Each advertising campaign is subject to approval by the Operator publisher network.
18. If changes are made to the website, services, content covered by an advertising campaign, the Operator must be notified immediately. In such a case, the Operator shall not be held liable if the changes have been made of which he has not been informed within a reasonable time before the changes were made. The Operator shall not be liable if it is not possible to adapt the Services to the changes.
19. Notification of changes should be made through the notification system or by e-mail.
20. If any kind of malware is detected, e.g. exploits, hijackers or viruses, the account will be disabled and the User will not be entitled to a refund. The above rules shall also apply in the situation of detecting activity by entities whose accounts have been blocked.
21. There is no entitlement to reimbursement of the Fee in the situations described above.
22. Campaign-related information and materials will be subject to removal if:
    1. they relate to a project that has been proven to be a fraud;
    2. the project is no longer active;
    3. the type of activity has been changed and the content does not reflect the current actual activity.
23. If any of the aforementioned conditions are met and the content will be deleted. Operator is in no way responsible and a refund will not be possible.
24. If the publisher deletes campaign-related information and materials delivered to his website through the Operator service, the publisher is required to notify Operator in regards to the deletion as well as the reason behind the decision.
25. If the publisher does not provide a valid reason for deleting the article, he will be required to fully refund the cost of the said article to Operator. Valid reasons for article deletion include:
    1. the project was proven to be a scam;
    2. the project is no longer active;
    3. the domain of activity has been changed and the content is no longer reflecting the current activity of the advertiser.
26. If the publisher does not refund the cost of the article he deleted, its account will be locked.
27. All campaigns on Operator are served, tracked, and reported by Operator. For campaigns that involve third-party serving/tracking, accounting may be beyond Operator's control.
28. The data generated by the campaign will only be available for 1 year, but no longer for the duration of the Agreement.

29. After this time, this data will be automatically deleted from the user's account. The user is solely responsible for downloading and saving this data if the user wishes to do so.
30. Before starting an advertising campaign, the required Fee must be paid according to the offer of the Operator.
31. Information on how to pay the Fee is provided via account.
32. In order to use selected services (such as advertising), the User must register.
33. In order to receive a bill or an invoice, all the necessary customer data must be provided.
34. The Operator may contact the User in order to complete the profile. If the User refuses to provide the necessary details, the campaign order shall be rejected.
35. The invoice and the payment document will be forwarded to the recipient electronically, at the e-mail address indicated.
36. Services will commence as soon as payment is received and accounted for.
37. Payments and settlements shall be made from the funds held in the deposit of the relevant User.
38. The Operator accepts deposits in the following cryptocurrencies: Xads
39. The User may only fund the deposit with cryptocurrencies accepted by the Operator.
40. If you wish to make deposits in other cryptocurrencies, please contact the Operator first or use an external provider.
41. All Fees are subject to change at any time. It is recommended that you always check the Fee before placing an order.
42. After the service has been requested, a Fee will be charged in accordance with the price list. The Fee will be charged from the funds accumulated within the deposit. In case of insufficient funds, the Operator shall not start the ordered service.
43. Funds held on deposit may be withdrawn at any time.
44. Information on how to create a deposit and the address of the wallet is provided by the Operator.
45. All bonuses granted may be used to purchase Services. Bonuses are not exchangeable for other funds. Unless otherwise stated, unused bonuses will be canceled.
46. The Operator may allow deposits in the form of cryptocurrencies. The Operator does not accept deposits in the form of currencies.
47. The User hereby indemnifies the Operator and the publishers (including their successors, directors, officers, employees, agents, assigns) against any liability as well as claims for advertising campaigns to the extent provided for in the Regulations, as well as in the event that the design, content proves to be unreliable, misleading or unlawful.
48. In cases where the law does not impose liability on the Operator, the Operator shall not be liable for any damages, including those resulting from loss of data, loss of use or loss of profit, or from the provision of services.

49. The Operator is not responsible in the event of loss of account access data by the User or their disclosure to other persons, as well as in the event of system failure or other technological failures, delay in delivery and / or failure to deliver the campaign, including, without limitation, difficulties with the publisher or the website. website, difficulties with a third party server or electronic failure, errors in content or omissions in the URL.
50. Complaints may be submitted in writing to the Operator's address; electronically, via the address contact@blockchain-ads.com
51. The complaint is examined within 14 days from the date of its receipt.
52. The complaint should contain the following information: identification data of the claimant (e-mail address provided during account registration), description of the reported problem, indication of the date of the problem (day, month, year).
53. If the complaint does not contain the information necessary for its consideration, the Operator will ask the person submitting the complaint to supplement it to the extent necessary, and the 14-day period then runs from the date of delivery of the completed complaint.
54. The response to the complaint is sent only to the e-mail address assigned to the User's account.
55. In the event of an appeal against a decision issued on the complaint, the above provisions shall apply accordingly.
56. The law applicable to the Agreement and disputes arising from the Agreement is St. Vincent and the Grenadines law.
57. Any disputes related to the Services provided to entities with the status of consumers will be settled by the competent St. Vincent and the Grenadines common courts.
58. An entity with the status of a consumer has the option of using an out-of-court complaint and redress procedure before the Permanent Consumer Arbitration Court.
59. Information on how to access the above-mentioned. The mode and procedures for resolving disputes can be found at the following address: https://gdpr-info.eu/, in the "Settlement of consumer disputes" tab. A user who is a consumer may also use the EU ODR internet platform, available at the following internet address: https://gdpr-info.eu/chapter-3/. Detailed information on the application procedure can be found here. The operator may attempt to settle the dispute amicably with the User running a business through an independent mediator, after prior consent to mediation.
60. If the User requests a mediation proposal and the Operator accepts this proposal, the mediation will be conducted by a mediator or mediators from the Wielkopolska Center for Arbitration and Mediation at the Wielkopolska Chamber of Commerce and Industry, in accordance with the mediation regulations applied by the Center. The operator will bear a reasonable share of the total mediation costs, which will be agreed by the parties from time to time.
61. The Operator informs that in connection with the use of electronic services, users remain exposed to threats, min. as:

1. the operation of spyware;
2. spoofing for phishing purposes;
3. computer viruses;
4. spam.

62. Threats concern not only computers, but also other portable devices, e.g. smartphones, tablets.
63. Spyware is one that can be covertly installed on the user's device, e.g. by accessing a crafted website or running a file sent via e-mail. It can monitor / send to the attacker both the data on the device and the user's actions: mouse movements, text typed from the keyboard, start preview / eavesdropping from the camera and microphone.
64. Phishing is the placing on the Internet of fake websites imitating the original ones and forcing users to log into them, e.g. by sending a specially prepared e-mail message that pretends to be a message from an authentic institution or person. The goal is to intercept access data to the service (login, password).
65. A computer virus is a malicious software that spreads by saving an infected file on a data carrier, e.g. a hard drive, USB flash drive. The purpose of the virus is to steal or delete data, disrupt or take control of the device. Most often, infection with a computer virus occurs after downloading files from an untrusted Internet source or opening an attachment in e-mail.
66. Spam is unsolicited or unnecessary electronic messages that are sent to multiple recipients simultaneously. They often carry computer viruses, spyware, and links to malicious websites.
67. In order to ensure safe use of the Internet, each user should:
    1. Take care of the safety of the device used. In particular, the device should have an antivirus program with an up-to-date virus definition database, an up-to-date and secure version of the web browser and an enabled firewall.
    2. Periodically check whether the operating system and programs installed on the device have the latest updates, because the attacks use errors found in previously installed software versions.
    3. Secure access data to services offered on the Internet - e.g. logins, passwords, PINs, electronic certificates, etc. such data should not be disclosed or stored on the device in a form that allows easy access and reading.
    4. Be careful when opening attachments or clicking links in messages that you did not expect, e.g. from unknown senders. In case of any doubts, it is worth contacting the sender.
    5. Use anti-phishing filters or other tools that verify that the displayed page is not phishing.
    6. Only download and install files from trusted sources.
    7. Set up a secure and hard-to-break password for accessing the network (Wi-Fi). It is also recommended to use trusted standards for encryption of Wi-Fi wireless networks, such as WPA2.

8. Control physical access to devices.

68. The Operator pays due attention to the protection of privacy.
69. Using the Services, including registration, requires providing data, including personal data.
70. The data controller of the User's personal data is the Operator.
71. Before using the Services, please read the rules for the processing of personal data available in Privacy Policy.
72. The business user (hereinafter referred to as the "Client") commissioning the Operator to provide advertising services (such as website traffic measurement) shall ensure that the users whose activity is to be monitored and about whom information is to be collected by the Operator in order to provide the commissioned service have given all necessary consents as required by law, as well as that they have been adequately and sufficiently informed about the Operator's activities. The Client shall be liable to the Operator for all damages suffered by the Operator if the Client fails to fulfill its obligations under this agreement, in particular the Client shall reimburse the Operator for the amounts paid by the Operator on account of penalties imposed on it by public authorities and compensation paid.
73. The Operator is entitled to amend the Regulations in the event of:
    1. changes in legal regulations or their interpretation;
    2. the imposition of certain obligations by state authorities;
    3. changes in fees;
    4. organizational changes, including those related to the operation of the Software or User service;
    5. technological and functional changes;
    6. changes in the scope of the Services or functionalities provided, including the introduction of new ones;
    7. editorial changes.
74. The amendment to the Regulations becomes effective within 15 days from the moment of notification of the changes and the availability of the new version of the Regulations.
75. The Operator will inform about the change in the Regulations and the possibility of accepting the change during the first login to the account, from the moment the changes come into force.
76. The new version of the Regulations will be published on the Blockchain-Ads.net website and sent to the e-mail address assigned to the account.
77. The Operator reserves the right to amend the Regulations without observing the 15-day deadline, with immediate effect, in the event of:
    1. when the introduction of changes results from a legal obligation or a decision of the competent authority, and the necessity to introduce the required changes makes it impossible to comply with the above-mentioned 15-day notification period;
    2. the change is necessary due to the need to counter fraud, malware, data breaches or other cybersecurity threats.

78. The changes may be accepted or not. In the absence of express acceptance of the new version of the Regulations, the first action performed after the amendments come into force shall be deemed to consent to the provision of Services under the new rules.
79. In the event of non-acceptance of the changes, in order to terminate the Agreement, the Operator must be notified immediately, not later than within 15 days from the announcement of the changes, via e-mail contact@blockchain-ads.com.
80. Termination of the Agreement in the above-mentioned mode takes effect 15 days after notification of the changes to the Regulations.
81. The User has the right to terminate the Agreement with a 30-day notice period.
82. The Operator has the option to terminate the Agreement with a 30-day notice period in the event of repeated breaches of the Regulations.
83. These Regulations are available in the English version, available at the following internet address: https://github.com/Blockchain-Ads/Blockchain-ads/blob/main/documentation/terms%26conditions.pdf
84. If any provision of the Regulations is considered invalid by a final court decision, the remaining provisions shall remain in force.
85. The Regulations are valid from 01.01.2022

ADVERTISING POLICY & RULES

1. Since high-quality advertisements help to maintain the standard of the network, but also increase advertisers' conversions, advertising material should be prepared diligently.
2. General rules for advertisers:
    1. Advertising content should comply with the law and the guidelines of the competent authorities. In particular, it is prohibited to advertise illegal products or services.
    2. Advertising content should be consistent with good morals and must not offend or discriminate against any social or ethnic group.
    3. Vulgar content and nudity are prohibited.
    4. Advertisements should be prepared with due care, i.e. meet the aesthetic requirements and not overload the website.
    5. Projects advertised online should work, provide valuable content and not be a scam or other type of scam.
    6. Abuse and deception of our or other advertising networks is prohibited.
    7. Landing pages that are blacklisted or contain any malware (virus, exploit, malware, hijack) may not be advertised on the network.
    8. Content in advertisements should be consistent with the actual product or service advertised. In addition, it is forbidden to advertise reflinks to websites, which in their regulations prohibit such advertising.

3. In case of non-compliance with these rules, the Operator shall not be held responsible and may refuse to provide services or cease to provide them. Money spent on campaigns is not refundable.
4. All advertising formats are subject to review and approval. The Operator reserves the right to reject any campaign without giving any reason.
5. Rules regarding ad formats:
    1. Acceptable ad formats are .jpg, .png, .gif in size max 0.5MB. In the case of .gif extensions, remember to optimize the file so that all transitions are smooth and do not overload the website.
    2. HTML ads packed in .zip extension are acceptable. The packages should contain all elements inside and no externals are allowed.
    3. It is forbidden to place in the advertisement direct links to pages with popup and popunder or banners without permission of the adserver operator.
    4. The use of iframes, popups and popunder is prohibited. These formats are only used in a few specific cases and may be approved with prior approval. Requests should be sent to contact@blockchain-ads.com. Repeated addition of these formats, despite rejection, will result in a ban.
6. Any attempt to manipulate the user, tracking, frame-breaking codes will result in a lifetime ban, which cannot be appealed. This also applies to ads that are blocked by your browser, firewall and antivirus.
7. The user may use the media plan service. All payments for the creation of a media plan should be paid before the service is provided and are non-refundable. Should the User wish to use their own media plan they should make an appointment with a member of the team by contacting contact@blockchain-ads.com. Pre-payments for the plan should be made before the plan is executed. These are partially refundable if the User cancels part or all of it before the compliance procedure begins and if the publisher decides to reject the material during the compliance procedure, does not take any action on the requested activities and does not issue a payment document for them. The publisher, after publishing the content, may remove it if it turns out that the advertised project is a fraud, is not active or the published content is incorrect and does not reflect reality. The advertiser may demand a refund if the above conditions are not met.
8. Repeatedly adding a campaign that has been rejected may result in your account being permanently banned. Additionally, if a banned user keeps creating new accounts to circumvent the restriction, all their accounts will be banned for life. You may file a complaint in accordance with the User Agreement available at https://github.com/Blockchain-Ads/Blockchain-ads/blob/main/documentation/terms%26conditions.pdf
9. Neither Operator nor the participating parties will be liable in any way for any damages resulting from the use of the software provided, including, but not limited to, advertising campaign errors and their consequences, website and code malfunctions, non-delivery/incomplete campaign delivery and any difficulties in its operation, technical failures and their consequences, delays, lack of access to the advertising system and other unforeseen difficulties.

10. Operator reserves the right to change any point of the terms and conditions and at any time without notice to you, who are required to keep this agreement under constant review.
11. In matters not covered by these Policy, the user agreement shall apply.

WEBSITE ACCEPTANCE POLICY

1. This document describes the rules for acceptance of parties and provision of services by the Operator. The User is obliged to become familiar with the content of the rules described below.
2. The Operator informs that it will only accept websites that are suitable for hosting advertising formats.
3. The Operator may request access to your Analytics account to verify the quality and authenticity of your traffic if it reasonably suspects that the data is fraudulent.
4. All Users who wish to use the Operator's services must comply with the following rules regarding websites and content:
    1. The website, as well as links and content, must not violate laws, guidelines of competent authorities.
    2. Users may not be asked to click on or be directed to any website or activity containing illegal content, illegal activities, harmful content, malware, or websites operated by entities competing with the Operator or promoting the activities of entities competing with the Operator.
    3. Traffic on the website should not be motivated by rewards for the user's presence or any other activity performed by him/her on the website.
    4. The site should not be involved in any illegal activity that may harm the welfare of the user or cause any financial loss by promoting suspicious, nefarious, spam or fraudulent projects.
    5. The site should not incite visitors to hatred, racism, violence or any activity that may cause moral or physical harm.
    6. Banners must be placed in high visibility areas (above the fold). Banners must not be hidden or distorted in any way, shape or form.
    7. Banners must be placed individually in the chosen location. Placing other banners together with banners from the Operator is prohibited.
    8. A banner must not be displayed on any page other than the one for which it has been approved.
    9. It is prohibited to artificially generate traffic, including buying traffic from other sources (advertising networks or other websites), which will then be sent to our advertisers' websites through their banners.

10. Website refreshment is prohibited in order to increase the number of times you see the banners displayed.

5. The Operator reserves the right not to start the service, discontinue the service and delete the website, if the website uses any kind of false, motivated or purchased traffic or unethical methods to generate income. In such a case, the Operator is not liable and the revenue from that account will be removed.
6. The above provision includes but is not limited to: autosurfs, iframes, bots, proxies, auto-hit services, traffic exchange systems.
7. Types of websites that will not be accepted on network:
    1. Sites containing or linking to any form of illegal activities;
    2. Sites with inappropriate or violent content and/or vulgar language;
    3. Sites promoting any type of hate-mongering (i.e. racial, political, ethnic, religious, gender-based, sexuality-based, personal, etc.);
    4. Sites that participate in or transmit spam using any kind of online means;
    5. Sites promoting any type of illegal substance or activity or sites with illegal, false, or deceptive investment advice and money-making opportunities;
    6. Sites that are using free domain names;
    7. Sites that don't have a unique design, that are filled with ads, that have more than 1 popunder and/or ask users to click on ads;
    8. URL Shorteners;
    9. Faucet websites;
    10. Websites with pornographic content;
    11. Websites created with the intention of sending bots/fake traffic to our network;
    12. Websites with no original content;
    13. Websites generated on platforms like Wordpress or Blogspot;
    14. Pay to click websites;
    15. Automatic/manual traffic exchanges;
    16. Any website that has incentivized traffic;
    17. Any website that, after it was reviewed by our team, wasn’t deemed suitable for our Publisher program;
    18. Websites that represent a coin, ICOs, or projects that raised funds from the community.
8. If a site is rejected, you may report the situation and submit a request for reconsideration.
9. The operator reserves the right to refuse to include any website in the display network, without giving a reason for its actions.
10. The Operator reserves the right to change the website acceptance policy. You are required to comply with any changes to the website acceptance policy within 2 days of the update and are required to read this page periodically.
11. This version is effective as of 01.01.2022 r.

Data Processing Agreement Definitions and Interpretations For the purposes of this Agreement, capitalized terms shall have the following meanings, unless defined elsewhere in the Agreement: “Business Day” shall mean any day except any Saturday, Sunday or a public

holiday in the respective countries of incorporation of the Parties to this Agreement; “Competent Data Protection Authority” shall mean the competent data protection authority, which, by way of example, could be the St. Vincent and the Grenadines Data Protection Authority. “Data Protection Legislation” shall mean all applicable data protection legislation, including the GDPR, any national data protection legislation, and any regulations, mandatory guidelines or any other mandatory codes of practice issued by any Competent Data Protection Authority, each as amended from time to time; “GDPR” shall mean Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as amended from time to time; “Main Agreement” shall have the meaning given to it in clause 2.1. of this Agreement; “Personal Data” shall have the meaning given to it in clause 3 of this Agreement. For the purposes of this Agreement, the terms “controller”, “processor”, “data subject”, “process”, “processing” and “data breach” shall have the meanings attributed to them in the GDPR. Purpose of this Agreement The Data Controller and the Data Processor are parties to one or more (concluded in parallel or by way of prolongation) agreements relating to the provision of advertising services by the Data Processor to the Data Controller (the “Main Agreement”). The purpose of this Agreement is to determine the roles and responsibilities of each Party during the provision of the services under the Main Agreement in order to ensure the Parties' compliance with the applicable Data Protection Legislation. Personal Data, Data Subjects, Processing Operations The Data Processor shall process on behalf of the Data Controller the following types of personal data of the following categories of data subjects: IP addresses of end users of the Data Controller Geographical coordinates (if applicable) of end users of the Data Controller information on terminal devices information on visited services (the “Personal Data”). The Data Processor shall process the Personal Data on behalf of the Data Controller for the purpose of the provision of the services under the Main Agreement. The Data Processor may not process Personal Data in a way that is incompatible with the purpose under this Agreement in relation to the Main Agreement as set out above. Term and Termination This Agreement shall commence on the date it is signed and shall continue in full force and effect until the expiry or termination for any reason of the Main Agreement on which date this Agreement shall automatically terminate without liability. Upon termination of the Agreement the Data Processor shall proceed in accordance with clause 5.15 of this Agreement. Obligations of the Data Processor The Data Processor shall process Personal Data only for the purpose of the Main Agreement. The Data Processor may not process Personal Data for its own purposes. The Data Processor shall process Personal Data in accordance with the instructions of the Data Controller and in compliance with the Data Protection Legislation. The Data Processor shall immediately inform in writing the Data Controller if the Data Processor believes that any of the instructions of the Data Controller violate the Data Protection Legislation. The Data Processor shall keep a written record of all categories of processing operations carried out on behalf of the Data Controller. This record shall contain: the name and contact details of the Data Processor, of each manager acting on behalf of the Data Processor and, where appropriate, of the representative of the Data Controller or the Data Processor and the data protection officer; the categories of processing operations carried out on behalf of the Data Controller; when applicable, personal data transfers to a third country or international organisation, including the identification of the said third country or international organisation and, in the case of transfers indicated in Article 49, Section 1, paragraph 2 of the GDPR, documentation on appropriate

safeguards. The Data Processor shall not disclose Personal Data to third parties, unless (i) to its sub-processors, (ii) with the express prior written consent of the Data Controller or (iii) when legally acceptable. For the avoidance of doubts, the Data Processor´s affiliates and subsidiaries shall not be considered third parties. The Data Processor may disclose Personal Data to other processors working for the Data Controller, pursuant to the Data Controller's instructions. In this case, the Data Controller shall identify, in writing and in advance, the entity Personal Data shall be disclosed to, the Personal Data to be disclosed, and the security measures to be applied for the disclosure. The Data Processor shall obtain Data Controller's prior consent to transfer Personal Data to an international organization or a third country. The obligation to obtain the consent applies in particular to entrust the processing of Personal Data to Sub-processors. The Data Processor has the right to engage sub-processors on condition that each of them will observe the binding regulations on personal data protection. In case of a planned entrusting the data processing to another sub-processor, the Data Processor shall notify the Data Controller in writing with at least 10 (ten) Business Days in advance, indicating the processing operations to be subcontracted to the sub-processor, and clearly and unambiguously indicating the sub-processor and its contact details. If within 10 (ten) Business Days of receipt of the notification, the Data Controller notifies the Data Processor in writing of any objections on reasonable grounds to the proposed appointment: The Data Processor shall cooperate with the Data Controller in good faith to make available a commercially reasonable change in the provision of the data processing services agreed upon under the Main Agreement; If such a change cannot be made within 90 (ninety) days from the receipt of the notification from the Data Controller by the Data Processor, the Data Controller may, by a written notice provided to the Data Processor, terminate with immediate effect the Main Agreement to the extent that it concerns services which require the use of the proposed sub-processor. The sub-contractor shall be equally obliged to comply with the obligations set out in this Agreement for the Data Processor and the instructions issued by the Data Controller. The Data Processor shall regulate its contractual relationship with the sub-contractor so that the sub-contractor is subject to the same conditions (instructions, obligations, security measures, etc.) and the same formal requirements for adequate processing of Personal Data and guarantee the rights of the data subjects. The Data Processor shall maintain the duty of secrecy regarding the Personal Data, even after the termination of the Main Agreement. The Data Processor guarantees that the individuals authorized to process Personal Data expressly undertake in writing to respect the confidentiality of the Personal Data and to comply with the relevant security measures, of which they shall be duly informed. The Data Processor shall keep documentation accrediting compliance with this obligation available for the Data Controller. The Data Processor guarantees that the individuals authorized to process Personal Data have the necessary data protection training. The Data Processor shall assist the Data Controller in meeting its obligations in relation to data subjects' requests to exercise rights (i) to access, rectification, erasure and object; (ii) to restriction of processing; (iii) to data portability; (iv) in relation to automated decision making and profiling. The Data Controller shall reimburse the Data Processor for all reasonable costs and expenses incurred with regard to such assistance. When data subjects exercise or declare their wish to exercise their rights under items (i), (ii), (iii) and (iv) above before the Data Processor, the Data Processor shall notify the Data Controller immediately but in any event not later than 72 (seventy-two) hours following the receipt of the request. The notification shall be

accompanied by other information (if provided and/or available) that may be relevant to resolve the request. The Data Processor shall notify the Data Controller without undue delay and in any event before the maximum period of 48 hours of any breach it is aware of to the security of the Personal Data it holds, together with all relevant information to document and report the incident. The following minimum information shall be provided, if available: description of the nature of the personal data security breach including, when possible, the categories and approximate number of data subjects affected, and the categories and approximate number of personal data records affected; the name and contact details of the data protection officer or another point of contact to obtain more information; description of the possible consequences of the personal data security breach; description of the measures adopted or proposed to remedy the personal data security breach including, if appropriate, the measures adopted to mitigate possible negative effects. If the above information cannot be provided simultaneously, the information shall be gradually provided without undue delay. The Data Processor shall support the Data Controller in sending prior consultations to Competent Data Protection Authorities, when appropriate. The Data Processor shall support the Data Controller in conducting data protection impact assessments, when appropriate. The Data Processor shall provide the Data Controller with all the information necessary to demonstrate compliance with its obligations under the Data Protection Legislation. The Data Processor shall allow the Data Controller to carry out audits and inspections. The Data Controller is entitled to conduct an audit/inspection at any time, in particular when the obligation to conduct an audit/inspection has been imposed by the supervisory authority or the conduct of an audit/inspection is necessary to explain the identified breach of Data Processor´s obligations under this Agreement. The Data Controller shall notify the Data Processor about the intention to conduct an audit/inspection at least 3 Business Days before the planned start of the audit/inspection. The notification should indicate the exact scope, date and persons authorized by the Data Processor to conduct the audit/inspection. The audit/inspection may be conducted by an independent auditor mutually agreed by the Parties.. The parties agree on the duration of the audit not longer than 7 working days, unless a longer time is necessary due to the purpose of the audit. In such case, the parties agree on the maximum duration of the audit. The audit ends with a protocol, which contains, in particular, the necessary scope of possible changes in personal data processing. The inspection may be carried out by obliging the Data Processor to answer the questionnaire. The questionnaire may be sent to the e-mail address indicated in clause 7. The Data Processor shall implement appropriate technical and organisational measures to: ensure a level of security appropriate to the risk involved in order to protect the Personal Data from unauthorized use, alteration, access or disclosure, loss, theft, and damage; ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; test, assess and evaluate the effectiveness of technical and organisational measures implemented for ensuring the security of the processing of the Personal Data; pseudonymise and encrypt the Personal Data, as appropriate; prevent a personal data security breach. The minimum technical and organizational measures to be provided by the Data Processor are listed in Attachment No. 2. The Data Processor shall promptly delete all Personal Data provided by the Data Controller in its entirety from its systems and destroy any copies it made of the Personal Data after completing the service, unless and to the extent that the Data Processor is

required to retain copies in accordance with the applicable Data Protection Legislation. Obligations of the Data Controller The Data Controller shall provide the Personal Data or otherwise make the Personal Data available to the Data Processor. The Data Controller shall, at the time when Personal Data is obtained, provide the data subjects will all information about the collection and processing of the Personal data and shall obtain any consent (where necessary) of data subjects as required by the GDPR and any other applicable Data Protection Legislation. The Data Controller shall supervise the processing operations performed by the Data Processor. The Data Controller may issue instructions about the type, scope and method of processing of the Personal Data in writing or send to the e-mail address indicated in clause 7 of this Agreement. Contact Point Each Party shall nominate the following contact person within their organisation who can be contacted in respect of queries, complaints or notifications of any kind whatsoever regarding this Agreement or the Data Protection Legislation: Miscellaneous In the event of any conflict between the terms of this Data Processing Agreement and any provision of the Main Agreement and any other agreement between the Parties, this Data Processing Agreement shall take precedence. Notwithstanding the governing law of the Main Agreement, this Data Processing Agreement shall be governed by and construed in accordance with the St. Vincent and the Grenadines law. All disputes, controversy, or claims arising out of or in connection with this Data Processing Agreement shall be subject to the exclusive jurisdiction of the St. Vincent and the Grenadines court(s). The provisions of this Agreement are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision and the rest of this Agreement shall remain in full force and effect. Any amendment to this Agreement must be made in writing upon mutual agreement by the Parties. For the purpose of this Agreement “writing”, “in writing” and “written” includes handwritten signatures, signatures produced by mechanical or digital means (such as scan, digitally scanned and stored signature inserted into [digital] document, etc.) as well as qualified electronic signatures. Also, for the avoidance of doubt, transmission/exchange in electronic format (for example scanned documents sent by email) do fulfill the form requirement. The written form requirement in this clause may only be waived by respecting the same written form requirement. Attachment No. 1 Minimum technical and organizational measures for personal data security: implementation of a written procedure for personal data protection, which regulates the principles of personal data protection in the processing entity; implementation of a procedure for safe use of IT resources; covering employees or co-workers with trainings in the scope of personal data protection and safe use of IT resources; processing of personal data only after prior written authorization to process the data; covering all persons acting on behalf of the processor with a written obligation to keep secret the information obtained within the framework of providing support services to the Data Controller; processing of the entrusted data in a secure area, covered by access control, physical protection or CCTV video surveillance; use by each employee/co-workers of a separate, unique access account to IT systems in which personal data are processed; applying a policy of strong passwords, forcing a change of passwords and blocking accounts; encrypting mobile devices that process personal data; centrally managed and controlled remote access to personal data; IT systems and software for processing personal data are regularly updated, verified for vulnerability and protected by antivirus systems; protection against unauthorized

access to systems and networks through a firewall, as well as using antivirus to preventaccess to malicious websites.