

Privacy Policy

We respect your privacy and are committed to protecting your privacy rights. Please take the time to read our Privacy Policy carefully. We want to be clear about how we use information, and about how you can protect your privacy. To ensure transparency, this Privacy Policy describes our information-handling practices when you access Data Whale mobile application ALGA (“The Application”) and our services, as defined below.

If you have any questions, please feel free to contact us at [info@datawhale.online].

References in this Policy to “Data Whale”, “we”, “our” or “us”, are to [COMPANY NAME] and references to “you”, “your”, “customer” or “user” are to the person who is a user of Applications. All the definitions used in this Privacy Policy shall have the same meaning as in our Terms of Service [CLICKABLE] unless this Policy sets a different meaning.

By accessing, downloading, connecting a Connected Wallet to or using The Application you signify acceptance to the terms of this Privacy Policy. Where we require your consent to process your personal information, we will ask for your consent to the collection, use, and disclosure of your personal information as described further below.

IF YOU DO NOT AGREE WITH THIS POLICY PLEASE UNINSTALL THE APPLICATION AND CEASE USING OUR SERVICES IMMEDIATELY.

1. Our Status

- a. We will act as a data controller in relation to personal information about you that may be either provided by you or collected by us.
- b. As a data controller, we will solely determine the purposes and means of the processing of your personal information.

2. How We Use Your Personal Information

- a. **We never collect your wallet's private keys or passphrases and never have access to your wallet because none of your private keys ever leave local storage of your device.**
- b. In this Section 2 we have set out:
 - i. the general categories of personal information that we may process;
 - ii. the purposes for which we may process personal information; and
 - iii. the legal basis of the processing.
- c. Please note that not all the information you provide to us is personally identifiable information according to the applicable law.
- d. **Usage Data.** We may process information about your use of The Application ("usage data"). The usage data may include:

- i. your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and navigation paths, as well as information about the timing, frequency and pattern of your use;
- ii. your device number, device id or unique identifier, device type, and unique device token, operating system and applications used, application crash-data, application version, device identifiers such as IDFA (Identifier For Advertisers), Android ID (Android device), referrer URL (Playstore), Google Advertiser ID, device model;
- iii. local storage files.

The source of the usage data is our analytics tracking system and your usage of The Application. This usage data may be processed for the purposes of analysing the use of The Application and to keep you signed in on The Application. The legal basis for this processing is your consent and our legitimate interest, namely monitoring and improving The Application and our services.

- e. **Account data.** We may process your account data (“account data”). The account data includes only the **public** wallet address of your Connected Wallet.

The source of the account data is you. The account data may be processed for the purposes of providing you access to our services, ensuring the security of The Application and our services and

communicating with you. The legal basis for this processing is a performance of an agreement between you and us and/or taking steps, at your request, to enter into such an agreement.

- f. **Enquiry data.** We may process information contained in any enquiry you submit to us regarding The Application and/or our services (“enquiry data”). The enquiry data may be processed for the purposes of responding to your enquiry, offering, marketing, correcting any deficiencies in The Application and/or services and providing relevant services to you. The legal basis for this processing is a performance of an agreement between you and us and/or taking steps, at your request, to enter into such an agreement and our legitimate interest.
- g. **Customer relationship data.** We may process information relating to our customer relationships, including customer contact information (“customer relationship data”). The customer relationship data may include your name, your nickname, your contact details (phone number, social media handle, email address or other social networks or messengers identifiers you use to communicate with us) and information contained in communications between us and you.

The source of the customer relationship data is you. The customer relationship data may be processed for the purposes of managing our relationships with customers, communicating with customers, keeping records of those communications and promoting our

products and services to customers. The legal basis for this processing is our legitimate interest, namely the proper management of our customer relationships.

- h. **Correspondence data.** We may process information contained in or relating to any communication that you send to us (“correspondence data”). The correspondence data may include the communication content and your contact information (phone number, email address or other social networks or messengers identifiers you use to communicate with us).

The correspondence data may be processed for the purposes of communicating with you and record-keeping. The legal basis for this processing is our legitimate interest, namely the proper administration of The Application, our services and business and communications with users.

- i. **Interaction data.** We may process your transactions information when you interact with technically supported decentralized protocols, liquidity pools, smart contracts and/or blockchains and information you generate through The Application (“interaction data”). This data may include your transactions, requests, contributing your crypto assets to liquidity pools and other details of your interaction with decentralized protocols, pools, blockchains.

The source of this data is your activities at or through The Application. This data may be processed for the purposes of

providing relevant services to you. The legal basis for this processing is the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract.

- j. **Verification data.** We may process information when we verify your identity (“verification data”). This verification data may include your name, address, telephone number, e-mail address, date of birth, national identification number, government identification documents, and, if applicable, information regarding your bank account (such as the name of the bank, the account type and account number).

The source of this data is you. This data may be processed for the purposes of identity verification and the detection of money laundering, terrorist financing, fraud, or any other financial crime, and/or performance our obligations to verify the identity of our customers. The legal basis for this processing is the compliance with our legal obligation, the protection and assertion of our legal rights, your legal rights and the legal rights of others, the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract.

- k. **Access to face / fingerprints recognition.** At your sole discretion you may enable face or fingerprints recognition for your authentication via The Application. We do not process any biometric data, rather this data is processed by your mobile device and operating system of your device. We do not get direct or

indirect access to this biometric data, we only receive the response from your phone in the format true-or-false at our Application's authentication request. You may disable face or fingerprints recognition for your authentication on our The Application at any moment by changing setting of your biometric data (for iOS: go to Settings > Face ID & Passcode, for Android: go to Settings > Biometrics and security).

- l. **Local storage files.** We may use local storage files to keep you signed in on The Application if you choose so. You can delete local storage files from your device at any time by visiting your device's settings.
- m. We may process any of your personal information identified in this Policy where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis for this processing is our legitimate interest, namely the protection and assertion of our legal rights, your legal rights and the legal rights of others.
- n. We may process any of your personal information identified in this Policy where necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice. The legal basis for this processing is our legitimate interest, namely the proper protection of our business against risks.

- o. In addition to the specific purposes for which we may process your personal information set out in this Section 2, we may also process any of your personal information where such processing is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another individual.
- p. It is your sole decision whether to provide us with the requested information or not. However, if you choose to withhold requested information, we may not be able to provide you with access to The Application or the possibility to use our services. Depending upon the activity, some of the information that we ask you to provide is identified as mandatory and some as optional. Please do not supply any other person's personal information to us, unless we prompt you to do so.

3. Disclosing Your Personal Information

- a. We may disclose your personal information to our affiliates, our contractors and our service providers insofar as reasonably necessary for the purposes, and on the legal bases, set out in this Policy.
- b. We may disclose your personal information to our insurers and/or professional advisers insofar as reasonably necessary for the purposes of obtaining or maintaining insurance coverage,

managing risks, obtaining professional advice, or the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

- c. In addition to the specific disclosures of personal information set out in this Section 3, we may disclose your personal information where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person. We may also disclose your personal information where such disclosure is necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.
- d. If we are required by the applicable law (for example, you are a resident of the EEA zone, UK or Switzerland) and your personal information is to be transferred outside our country of incorporation ([JURISDICTION]) and/or the EEA zone, UK or Switzerland, we will ensure an adequate level of protection by any of the recognised methods of transfer, including but not limited to entry into the standard contractual clauses for the transfer of personal information to processors established in third countries.

4. General Processing

- a. Our processing means any operation or set of operations which is performed on personal information, such as collection, recording,

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, support, maintenance, etc. We do not make automated decisions, including profiling.

- b. We have implemented measures designed to secure your personal information from accidental loss and unauthorised access, use, alteration, and disclosure, but can not be held liable for the same.

5. Retaining and Deleting Personal Information

- a. We only retain your personal information for as long as it is necessary for us to use your information as described above or to comply with our legal obligations and legitimate interests. For instance, we may retain your data as necessary to meet our legal obligations, such as for tax and accounting purposes.
- b. We will retain your personal information no longer than 3 years from: i) your sign in to Applications, ii) the last delivery of our services to you, or iii) our last interaction with you related to your inquiry about The Application, our services or any other issues you have related to The Application or services, whichever is later.
- c. We will store your personal information that is used to send you promotional e-mails and/or newsletters or used in relation to your

support tickets. Such information will be stored and processed solely for this purpose until you withdraw your consent, where applicable, or unsubscribe from newsletters, but not longer than for 3 years after your last interaction with us.

- d. Otherwise, we either delete or anonymise the personal information collected. In case personal information was transferred to backup storage and, therefore, cannot be deleted, we continue to store it securely, but do not use it for any purpose. In all the other cases, we proceed with the deletion of personal information.
- e. Please be aware that any blockchain wallets, even if created or connected through The Application, cannot be deleted from the blockchain due to the technological specifics of blockchain networks and distributed ledgers.

6. Third Parties

- a. The Application may contain links to any other websites or services. Please note that we are not responsible for the privacy practices or the content of such websites or services, and you should review the privacy policy of each such website or service to make sure you are comfortable with it before providing any personal information.

7. Rights of European Users

If you located in the EEA zone, UK, Switzerland as a data subject (a person whose personal information is collected, stored and processed) you have several rights under data privacy laws:

- a. **Right of access.** You have the right to obtain confirmation if your personal information is being processed by us. If that is the case, you can access your personal information and the following information: (i) the purposes of the processing; (ii) the categories of personal information; (iii) to whom the personal information has been or will be disclosed; (iv) the envisaged period for which the personal information will be stored, or the criteria used to determine that period.

If you would like to have a copy of your personal information from us, we will provide it if (i) you prove your identity, (ii) it will not adversely affect the rights and freedoms of others. The first copy will be provided for free, for any further copies we may charge a reasonable fee based on administrative costs.

- b. **Right to rectification.** You have the right to demand that we correct without undue delay your personal information which we have in our systems if it is inaccurate or incomplete.
- c. **Right to erasure (“right to be forgotten”).** You have the right to demand that we erase your personal information, and we shall

erase it without undue delay where one of the following grounds applies: (i) this personal information is no longer necessary in relation to the purposes for which it was processed; (ii) you withdraw consent on which the processing is based, and where there is no other legal ground for the processing; (iii) you object to the processing and there are no overriding legitimate grounds; (iv) your personal information has been unlawfully processed; (v) your personal information has to be erased for compliance with a legal obligation.

- d. **Right to restrict processing.** You have the right to restrict us in the ability of processing your information where one of the following applies: (i) you contest the accuracy of your personal information and we are verifying it; (ii) the processing is unlawful and you want to restrict it instead of erasure; (iii) we no longer need your personal information, but you need it for establishment, exercise or defense of legal claims; (iv) you have objected to processing and we are verifying whether legitimate grounds override your request.
- e. **Right to data portability.** You have the right to receive your personal information which you provided to us in a structured, commonly used and machine-readable format and have the right to transmit those data to another company, where: (i) the processing is based on your consent or on a contract; and (ii) the processing is carried out by automated means.

Where technically feasible, you can demand that we transmit those data directly to another company.

- f. **Right to object.** You have the right to object to the processing of your personal information based on our legitimate interests. We shall no longer process your personal information unless we demonstrate compelling legitimate grounds for the processing or for the establishment, exercise or defense of legal claims.

Where personal information is processed for direct marketing purposes, you have the right to object at any time to the processing of your personal information for such marketing.

- g. **Right to withdraw consent.** You have the right to withdraw your consent for processing of your personal information at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

8. Changes to this Privacy Policy

- a. We may modify this Privacy Policy by providing notice of such changes, such as by sending you an email, providing notice through The Application or their newsfeed, or updating the “Effective Date” date at the bottom of this Privacy Policy. By continuing to access or use of The Application, you confirm your agreement to the modified Privacy Policy. If you do not agree to any modification to this Privacy Policy, you must stop using The

Application and our services, and delete The Application from your devices. We encourage you to frequently review the Privacy Policy to ensure you understand the terms and conditions that apply to your access to, and use of, The Application and our services.

9. Contact details

- a. If you have any requests concerning your personal information or any queries with regard to this Privacy Policy please feel free to contact us at [info@datawhale.online] or our mailing address below:

[COMPANY NAME]

[ADDRESS]

Effective Date: 26/08/2021