Privacy Notice

Date: 1st December 2023

Purpose

For the purposes of this Privacy Notice, Naumard Ltd., a company duly registered under the laws of Cyprus, with registered office in Arch Makariou III, 172, Melford Tower, 3027 Limassol, shall be referred to as,"**Company", "we", "Us", "us" or "We**".

The Company has adopted this Privacy Notice in order to inform and explain to you of its policies with respect to information collected as part of daily operations from where the services are offered directly by the Company's online and mobile web sites.

The Company shall collect Personal Data from a natural person (the "**Users**") who set up a User Account (as defined in the "**Definitions**" section below).

The Company uses privacy by default and privacy by design standards and undertakes to store your Personal Data in a secure manner and to process your Personal Data with all appropriate care and attention in accordance with the European Regulation 2016/679 "General Data Protection Regulation" (the "**GDPR**") and Cyprus law 125(I)/2018.

Scope of Privacy Notice:

This Privacy Notice shall apply to any use of the Platform and/or App (as all defined in the "**Definitions**" section), whatever the method or medium used. The Privacy Notice is used to explain the collection of Personal Data and rights of Users and discloses:

- What information we collect and why we collect it;
- Conditions at which we collect, keep, process and save information;
- How we use that information.

If you have any questions about this Privacy Notice, please contact us at: support@youhodler.com.

1. Definitions

For the purposes of this Privacy Notice, the terms hereunder have the following definitions assigned to them:

Adequate Country	means a country or territory that is recognized under EU Data Protection Laws as providing adequate protection for Personal Data;
AML	refers to Anti-Money Laundering;
AML Laws	refers to the 5th AML Directive, The CySEC Directive for the Prevention and Suppression of Money Laundering and Terrorist Financing;
Application or **App**	refers to the mobile application which is available on Android and iOS that bears the name "YouHodler" and which allows Users to access the services through their electronic device;
Cryptocurrency	means a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank;
CVM	refers to Cardholder Verification Method;

Consent	means any freely given, specific, informed and unambiguous indication of which the Data Subject, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him;
Cookie(s)	means a piece of information that is placed automatically on your electronic device's hard drive when you access the App(s) and which is listed in the Cookie Declaration available at:https://www.youhodler.com/cookies. The Cookie uniquely identifies your browser to the server. Cookies allow the Company to store information on the server (for example 1 language preferences, technical information, click or path information, etc.);u;
Data Controller	means the natural or legal person, which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data and who is in charge of this Processing. For the purpose of this Privacy Notice, the data controller is the Company;
Data Portability	means the right of the Data Subject to receive its Personal Data in a structured, commonly used and machine-readable format and the right to transmit those data to another controller without hindrance from the Company;
Data Subject(s)	means the natural or legal persons whose data is processed, i.e. in the context of this Privacy Notice, the Data Subject is the Visitor and the User of the Website and/or the Application;
Disclosure	means making Personal Data accessible, for example by permitting access, transmission or publication;
EU Data Protection Laws	means all laws and regulations of the European Union, the European Economic Area, their member states including (where applicable) the GDPR;
External Wallet(s)	means a Cryptocurrency wallet or wallets to which a User may elect to send Cryptocurrencies or from which a User transfers or receives Cryptocurrencies;
Fiat Currency(-ies)	means a centralized issued currency which is not backed by a physical commodity;
Force Majeure Event	means an act or event, whether or not foreseen, that: (i) is beyond the reasonable control of, and is not due to the fault or negligence of the Company, and (ii) could not have been avoided by the Company's exercise of due diligence, including, but not limited to, a labor controversy, strike, lockout, boycott, transportation stoppage, action of a court or public authority, fire, flood, earthquake, storm, war, civil strife, terrorist action, epidemies, pandemics, inability to obtain raw materials, supplies or equipment through its usual and regular sources, or any act beyond the Company's control;
GDPR	means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data);
KYC	refers to Know-Your-Customer;
Payment data	means data relating to your means of payment, including but not limited to payment which occurs by credit card, bank references, name of the owner of the account, card number, expiration date and other such data;
PCI-DSS	refers to Payment Card Industry – Data Secure Standards;

Personal Data	means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person as well as any Sensitive Data;
Personal Data breach	means a breach of security leading to the accidental or unlawful destruction, loss or alteration of – or to the unauthorized Disclosure of, or access to – Personal Data transmitted, stored or otherwise processed;
Platform	means the online platform which is available after providing login credentials at https://app.youhodler.com/sign-in and where the Services are offered by the Company;
Processing	means any operation with Personal Data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data. When referred in the past tense, this term is also referred to as “Processed” ;
Recipient	means a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a third party or not;
Sensitive Data	means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or activities, genetic data or biometric data processed for the purpose of uniquely identifying natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, data on the intimate sphere, social security measures, and data on administrative or criminal proceedings and sanctions;
Sub-Contractors	means natural or legal persons who are contractually bound with the Company to operate or maintain the Website or Application or offer any form of service offered by the Company within the Website or Application;
User Account(s	means the personal account created upon your registration with the Platform;
Visitor(s)	means any person visiting the Website who does not create a User Account nor makes use of the Services available on the Platform;
Website	means the website which is found at the following URL https://www.youhodler.com, and related domain extensions;
Website Content	means all features, texts, designs, layouts, wireframes, software, information, documents or content displayed on and/or technical information associated with the Website;
5th AML Directive	means Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

2. Data Controller and Processor

For the purpose of providing operational services and operating the Platform, your Personal Data will be collected and processed by Naumard Ltd. with a registered office at Arch Makariou III, 172, Melford Tower, 3027 Limassol, Cyprus.

3. Acceptance of this Privacy Notice:

By browsing the Platform, Visitors acknowledge that Naumard Ltd. may collect and Process certain amount of Personal Data that relates to them and that they agree to be bound by this Privacy Notice and to comply with all applicable laws and regulations. If a Visitor does not agree with this Privacy Notice, they should stop or refrain from using the Website.

Users acknowledge that Naumard Ltd. may collect and Process certain amounts of Personal Data that relate to them and that they agree to be bound by this Privacy Notice and to comply with all applicable laws and regulations.

In particular, the Consent for the Processing of Personal Data in accordance with this Privacy Notice is given once the User accepts the tick box affirming the User's Consent when using the Platform and/or downloading the Application.

Consent is also given when the User freely submits the Personal Data required to become a User to the Company. The User understands and agrees that the Company is free to use this Personal Data within the limit provided by law and this Privacy Notice.

If the Visitor or User does not agree with this Privacy Notice, they should not create an account on the Platform and become a User.

4. Information Collected

This Privacy Notice applies to all information that is received, when browsing our Website and/or when you send your Personal Data in order fulfill the on-boarding procedure for when you become a User on the Platform or the Application.

It is important to understand that we may request that you provide this Personal Data at different stages throughout your interaction with or use of the Platform. The Personal Data is collected from you through your own disclosure, automatically, or by third party service providers.

Collected Data from you

Visitors' / Users' Data - For the purpose of accessing the Platform services the following are collected : Cookies (provided the user accepted the Cookie Policy) found at https://www.youhodler.com/cookies ; the user's geographical location; type of browser that the user use; the user's server name; the user's IP address through which the user access the internet; the date and time the user access the Platform/Application or visit the Website; the pages the user access; the internet address of the web sites, if any, from which the user linked directly to the Platform/Application.

Registration Data - your phone number; your email address; country of residence.

KYC and AML Data - Personal Data collected for KYC purposes and in order to have the Services available on your User Account, including but not limited to: first name and surname, date of Birth, gender, address (full details), nationality, country of birth, country of residence, a photographic image of a document which you wish to present, valid Identity document (for facial comparison, visual authenticity and face comparison, image integrity, validation/comparison/consistency of data which can be matched with the Identity document, for police record purposes), selfie or video for facial similarity check, document extract (ID report), document extract (wealth), document extract (AML), document extract (residency or utility bill), recordings of video verification calls, documents whose content purports to verify your source of wealth and source of funds.

User Suitability Data - The User may need to answer questions and provide us with certain Personal Data in order for us to understand which Services are best suitable for you. This may include: basic suitability form based on your occupation, investment and cryptocurrency experience, answers to the questions regarding the origin of the funds, answers to the questions for advanced suitability, answers to the questions which measure the Risk level, proof of residency, proof of wealth, and watchlist Report.

Financial Data - Information relating to fiat currency account origin, fiat currency account address, fiat currency account details, fiat currency account balance, address(es) of your External Wallet(s), global balance in your User account at any given time, Cryptocurrency balance in your User account at any given time, fiat currency balance in

your User account at any given time, details of your User account at any given time, global balance in your External Wallet(s) (if required).

Transaction Data - Information related to execution of a transaction or on the use of the Company's support services, including cryptocurrency amounts, request date, details related to the Agreement (included content that you view, download or submit), billing information, User Account audit logs, User Account communication logs, User Account level, displayed Currency, Virtual Asset Service Provider (VASP) public address to which the Cryptocurrencies are sent, Originator (sender) information and required beneficiary (recipient) information of transactions, your External Wallets address, the digital assets located in your External Wallets, any details available regarding your External Wallets, and the balance available in your External Wallets (if required).

Credit Data - Data collected before using the services through the Platform, including your name and surname, your address, your date of birth, all the relevant information and documents about the seizable part of your income:

- all income of any kind;
- all labour income;
- all usufruct and their products/ all life annuities;
- all maintenance contributions;
- all pensions and benefits of all kinds intended to cover a loss of earnings or a claim arising from the right of maintenance, in particular pensions and capital allowances;
- a certificate of salary, if you are working as an independent, all the relevant information and documents proving your income, all the relevant information and documents about your wealth situation, the rent you pay for your accommodation, an extract of your rental lease agreement, the amount of all the taxes you pay to the tax authorities, an extract from your tax declaration, the amount of all the credits you have already obtained, an extract of the documents related to these credits, an extract from the debt collection register, and all the relevant information and documents about your expenses.

Sensitive Data- Sensitive Data as defined within this Privacy Notice which shall be collected only if at least one of the following cases make their collection and processing possible:

- the Data Subject has given explicit consent;
- for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorized by national laws providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;
- the Data Subject is physically or legally incapable of giving consent and there is a necessity to protect the vital interests of the Data Subject or of another natural person;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the Data Subjects;
- processing is under the control of an official authority or when the processing is authorized by Cypriot laws providing for appropriate safeguards for the rights and freedoms of Data Subjects;
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Collected Data automatically

Location Data – Information that is automatically collected via analytics systems providers to determine your location, including your IP address and/hor domain name, any internet address of the web sites from which you linked directly to the Application or Platform, your login information, browser type and version, date and time you access the Application, browser plug-in types and versions, operating system, and platform. This information is gathered in order to verify the User's location when providing proof of address.

Log Information Data – Information that is generated by your use of the Platform or Application that is automatically collected and stored by the Company. This may include, but is not limited to, device-specific information, location information, system activity and any internal and external information related to pages that you visit prior to the Platform.

Collected Data from third party providers

Bank Transaction Information and/or payment provider information - Information from the banks and/or payment providers you use to transfer money to the Company such as your basic personal information, your name and address, as well as your financial information such as your bank account details and where possible, card details when executing payment cards.

Advertising Data - Information from advertising networks, analytics providers and search information providers which are anonymized or de-identified information about you.

PEP and Sanction Screening information - Information collected and carried out by our AML third-party service providers or from public domain databases based on the extracted information of your identity document.

Please keep in mind that comments sections, forums, and other similar areas of our services are public. Any information posted in those areas is viewable and usable by anyone that has access.

5. Methods and Principles for Information Collected

- **Methods of Collection**

The Company uses different methods for collecting the Personal Data, such as the following:

Registration Forms

If you are offered the opportunity to enter a promotion, to become a member of the Web Sites, or to register, you must fill out certain registration forms on the Platform or Application in order to comply with AML and KYC policy. This requires you to fill out the registration form on the Platform.

Transactions and Activity

All your activity on the Platform or Application when making use of the Services is registered and collected in order to ensure that the Company is offering the services you want within the parameters that you set when making use of the Services.

Email and other voluntary communications

You may also choose to communicate with us through email, via the Platform or Application with our customer support agent chats, in writing Communications and responses to the customer support agents or compliance agents are considered to be explicit consent to Data collection and processing.

- **Principles of Collection**

While Processing Personal Data, the Company will respect the following general principles:

Fairness and lawfulness

When Processing Personal Data, the individual rights of the Data Subjects will be protected by the Company. Personal Data will be collected and Processed lawfully, in a fair manner, in good faith and must be proportionate to the objective.

We generally only process your Personal Data where we are legally required to, where Processing is necessary to protect your or another User's vital interests, where Processing is necessary to perform and enter into any contracts with you, where Processing is in our legitimate interests to operate our business and not overridden by your data

protection interests or fundamental rights and freedoms, or where we have obtained your consent to do so. To the extent that at least one of the above applies, Processing of Personal Data shall be considered lawful.

Restriction to a specific purpose

Personal Data collected shall be done for specific, explicit and limited purposes and not further processed in a manner that is incompatible with those purposes. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

Data minimisation

Personal Data handled by the Company should be adequate and relevant to the purpose for which they are collected and processed. This requires, in particular, ensuring that the types of Personal Data collected are not excessive to the purpose for which they are collected.

Transparency

The Data Subject must be informed of how his/her Personal Data is being handled by the Company. When the Personal Data is collected, the Data Subject must be informed of: the existence of the present Privacy Notice; the identity of the Data Controller; the purpose of the collection of Personal Data and its Processing; how, where and by whom the Personal Data is being processed; third-parties to whom the Personal Data might be transmitted.

Consent of the Data Subject

Personal Data must be Collected directly from the Data Subject concerned and the Consent of the Data Subject must be granted before Processing Personal Data. The Consent must be obtained in writing or electronically for the purposes of documentation. The Consent is valid only if given voluntarily. If, for any reason, the Consent of the Data Subject is not given before Processing, the Company should be informed in writing as soon as possible after the beginning of the Processing.

Personal Data can be Processed without Consent if it is necessary to enforce a legitimate interest of the Company. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims, any duties which may arise from any licensing obligations) or financial (e.g. valuation of companies as well as for carrying out the Services) nature. The Processing of the Personal Data is also permitted if national or foreign legislation requests, requires or allows it.

Accuracy

Inaccurate or incomplete Personal Data should not be kept on file and deleted, unless otherwise stated by legal provisions. The Personal Data kept on file must be correct and if necessary, it must be kept up to date.

Storage limitation

Personal Data should not be kept for longer than is necessary for the purposes for which it is being processed, unless otherwise required; personal data may be stored for longer periods in the event where the Company is obliged to maintain the data in order to comply with other obligations, for example to comply with the obligations deriving from the laws of Cyprus implementing EU 5th AML Directive, the amending law 188(I)/2007 on 'Prevention and Suppression of Money Laundering and Terrorist Financing' and any amendments and updates to this legislation.

Integrity and Confidentiality

Appropriate technical or organizational measures are put in place for Personal Data to be given appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using.

6. Use of Information Collected

The Company may use the collected Personal Data through its Platform or Application primarily for such purposes as:

- **Contract Performance and onboarding process**

The Personal Data serves to establish and verify the identity of users; opening, maintaining, administering and servicing users' accounts or memberships; processing, servicing or enforcing transactions and sending related communications; providing services and support to Users;

- **Compliance with legal obligations**

By browsing the Platform or Application as a Visitor and/or by using the Platform or Application as a User, you understand that the Company must respect the applicable laws and regulations and comply with any obligations which the Company is requested to comply with by virtue of any regulations, guidelines or laws which apply to the Services rendered through the Platform or Application, in particular the EU General Data Protection Regulation, the Cyprus data protection law 125(I)/2018 and law 188 (I)/2007 on Money Laundering (amongst other laws which are applicable to the Company) and any amendments to such laws and regulations.

- **Product and Service**

The Personal Data is used for improving the Platformor Application, including tailoring it to Users' preferences; providing Users with product or service updates, promotional notices and offers, and other information about the Company and its affiliates; responding to your questions, inquiries, comments and instructions.

- **Legitimate Interest**

By browsing the Platform or Application as a Visitor and by using the Platform or Application as a User you understand and expressly Consent that YouHolder has the legitimate interest to process Personal Data for security reasons, in particular to insure a legal and peaceful utilization of the Platform or Application in the full respect of the laws and suitable regulations, maintaining the security and integrity of the systems, and protecting our systems from fraud and unlawful access.

These Personal Data are collected and used to prevent potentially prohibited or illegal activities. These Personal Data are used in order to know who interacted with the Platform or Application and to ensure that there is no cyber-security threat and in order to have an initial verification of the potential User of the Platform or Application. If a cyber-security threat occurs at a particular moment, it would be possible to identify the whereabouts of the threat. In particular, we use your geographical location information in order to ensure that the Services will not be used in a country/area where it is expressly prohibited for the Platform or Application to be used in order to ensure that no legal action is taken against the Company.

We will collect only as much personal information as is needed for these specific purposes, and will not use it for other purposes without obtaining your consent.

We, or our advertising networks may also use cookies, tag, beacon, or other similar technology to serve you relevant advertisements and alert you to our content, even on other sites and services. This technology can also be used to collect and analyze aggregated information about our Users.

7. Protection of Information Collected

We work hard to protect our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. For example, we follow high industry standards and will always apply adequate technical and organizational measures for safety, we use computer safeguards such as firewalls and data encryption, we enforce physical access controls to our buildings and files, we do regular testing and evaluations on the effectiveness of technical measures, and we authorize access to personal information only for those employees who require it to fulfill

their job responsibilities. A further detailed list of the security and organizational measures taken by the Company is available under the Data Protection Addendum herein incorporated.

In the event of a Personal Data breach, the Company shall without undue delay, and where feasible, not later than forty-eight (48) hours after having become aware of it, notify the breach to the competent supervisory authority, unless said breach is unlikely to result in a risk to your rights and freedoms. If the breach is likely to result in a high risk to your rights and freedoms, the Company shall communicate this breach to you, if it is feasible, without undue delay.

Personal Data and data security is not solely dependent on the Company. You should protect the account information in your possession as well. When using our Services you play a vital role in protecting your own personal information. When registering with our Services, it is important to choose a password of sufficient length and complexity, to not reveal this password to any third-parties, and to immediately notify us if you become aware of any unauthorized access to or use of your account.

Furthermore, we cannot ensure or warrant the security or confidentiality of information you transmit to us or receive from us by internet or wireless connection, including email, phone, or SMS, since we have no way of protecting that information once it leaves and until it reaches us. If you have reason to believe that your data is no longer secure, please contact us at "support@youhodler.com".

8. Rights of User

Transparency and modalities

We try to facilitate access to information relating to the Processing of your Personal Data and other general information about data processing.

This Privacy Notice, together with the various articles and communications throughout the Application and/or Platform which you might have with us, try to answer in a clear and concise manner any enquiries or requests you might have in regards to Processing.

For security reasons, any communications from us will only come in written form from the in-app chat, Platform or via emails coming from the domain name@youhodler.com.

In case we have reasonable doubts concerning the identity of the natural person making the inquiry, we may request the provision of additional information necessary to confirm the identity of the Data Subject. We provide answers to requests within the month, however please take into consideration that this period may be extended when necessary and according to the complexity and number of the requests at the moment.

Information and access to Personal Data

You have the **right to request access** to or information about the Personal Data relating to you which are Processed by the Company.

Whenever you use our services, we aim to provide you with access to your personal information in your account. If that information is wrong, we strive to give you ways to update it quickly or to delete it unless we have to keep that information for legitimate business or legal purposes. When updating your personal information, we may ask you to verify your identity before we can act on your request.

Where provided by law and to the extent permitted by it, you, your successors, representatives and/or proxies may **(i) request erasure, correction or revision of your Personal Data; (ii) oppose the data Processing; (iii) limit the use and Disclosure of your Personal Data; and (iv) revoke Consent** to any of our data Processing activities, if the Company is relying on your Consent and does not have another legal basis to continue Processing the Personal Data.

If you request a limitation, erasure or correction of the Personal Data being Processed in connection with direct marketing purposes and decision-making, the Personal Data shall no longer be processed for such purposes; the Processing of the Personal Data will continue when our legal obligations compel us to and only to the extent permitted by law.

Right to Data Portability

You also have the right to receive your Personal Data, which you have provided to the Company in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Company.

This right can be exercised by contacting us through our contact form or writing to us at "support@youhodler.com" attaching a copy of your ID. If the request is submitted by a person other than you, without providing evidence that the request is legitimately made on your behalf, the request will be rejected.

The request is free of charge unless your request is unfounded or excessive (e.g. if you have already requested such Personal Data multiple times in the last twelve months or if the request generates an extremely high workload).

In such a case, the Company may charge you a reasonable request fee according to applicable laws. The Company may refuse, restrict or defer the provision of Personal Data where it has the right to do so, for example if fulfilling the request will adversely affect the rights and freedoms of others. The User hereby understands, acknowledges and accepts that the content of this section does not apply to the transaction data enlisted hereunder:

- the digital assets located in your External Wallet address;
- any details available regarding your External Wallet address;
- the balance available in your External Wallet address.

If we provide you with any mailings or other communication, you can always opt out of that communication.

You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, it's important to remember that many of our services may not function properly if your cookies are disabled.

Right to lodge complaint

The user has the right to make a complaint if the user feels his/her personal data has been mishandled or if the Company has failed to meet the user's expectations. Section 13 of this Notice specifies the relevant supervisory authority to which the user can file their complaint.

Automatic Decision-Making or Profiling

The Company does not make profiling based on automatic decision-making.

9. Do Not Track Signals

Some web browsers have settings that include "do not track signals." Our services are not currently engineered to respond to those signals from browsers.

10. Disclosure

We do not share personal information with companies, outside organizations ,individuals or other Recipients unless one of the following circumstances apply:

- With your consent. We will share personal information with companies, outside organizations or individuals if we have your consent to do so;

- For external Processing. We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Notice and any other appropriate confidentiality and security measures.

- For legal reasons. We will share personal information with companies, outside organizations or individuals (such as forensic experts and investigative service providers) if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to meet any (i) applicable law or regulation; (ii) in response to legal proceedings or enforceable governmental request; (iii) in response to a request from a competent law enforcement agency, national authority or self-regulatory association or agency; (iv) to detect, prevent, or otherwise address fraud, security or technical issues; (v) to protect against harm the rights, property or safety of our users or the public as required or permitted by law; or (vi) to

enforce the terms of any agreement.

- In case of a sale or asset transfer. If we become involved in a merger, acquisition or other transaction involving the sale of some or all of our assets including through bankruptcy, User information, including personal information collected from you through your use of our services, could be included in the transferred assets. Should such an event occur, we will use reasonable means to notify you, either through email and/or a prominent notice on the services.

- In aggregated form for business purposes. We may share aggregated, non-personally identifiable information publicly and with our partners we have a relationship with, advertisers or connected sites. For example, we may share information to show trends about the general use of our services.

11. Data transfers

The Company may also share your Personal Data or any Collected Data or processed by it with other entities. In any case where cross-border transfer is done, the Company ensures that an adequate protection is guaranteed for Personal Data to be transferred outside the European Economic Area (hereinafter referred to as the "EEA") or the United Kingdom using standard contractual clauses which are issued by the European Commission or binding corporate rules. The User acknowledges and accepts that the provision of the Service under the Terms may require the processing of Personal Data by sub-processors in countries outside the EEA.

If, in the performance of this Privacy Notice, the Company transfers any Personal Data to a sub-processor located outside of the EEA or the United Kingdom, the Company shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as:

- the requirement for the Company to execute or procure that the sub-processor execute to the benefit of the User standard contractual clauses approved by the EU authorities under EU Data Protection Laws;
- the existence of any other specifically approved safeguard for data transfers (as recognised under EU Data Protection Laws) and/or a European Commission finding of adequacy.

All Personal Data stored or processed by sub-processors is done in conformity with their privacy policy and privacy notice. A list of countries of data transfer countries and sub-processors is included under the attached Annex 1.

For the purposes of supporting the client with operations, you understand that your data will be transferred to the following entities:

YouHodler Italy Srl - Via del Lauro 9 20121 Milano

YouHodler SA - Avenue du Théâtre 7, 1005 Lausanne

Single Sign-On (SSO) Integration

We offer the option to log in to our services using your Google Sign-in or Apple ID account for your convenience. When you choose to use sign-in with Google Sign-in or Apple ID, we collect and process certain information from your Google account or Apple ID to create and manage your user profile. This information may include your name and email address.

By using Google Sign-in to access our services, you consent to the collection and processing of this information. We use this data solely for the purpose of user authentication and account management. We do not access or store any other personal information or sensitive data from your Google account.

Please note that the use of Google Sign-in is subject to Google's privacy policy and terms of service. We encourage you to review Google's privacy policies to understand how they handle your data.

In compliance with applicable data protection regulations, you have the right to revoke this consent at any time and request the removal of your account. You can do so by contacting our team at support@youhodler.com.

12. Third-Party Sites

Our Privacy Notice does not apply to services offered by other companies or individuals, including products or sites that may be displayed to you on this site. We also do not control the privacy policies and your privacy settings on third-party sites, including social networks.

13. Enforcement and Complaints

We regularly review our compliance with our Privacy Notice.

The Company hopes to be able to answer any questions or concerns you have about your Personal Data. You can get in touch with the Company at the postal address or email address given in section 18 herein.

You have the **right to file a complaint** if you feel your Personal Data has been mishandled.

You are encouraged to contact the Company about any complaints or concerns but you are entitled to complain directly to the relevant supervisory authority and data protection commissioner. When we receive formal written complaints, we will contact the person who made the complaint to follow up. The relevant data protection authority to which you may report are available here:

Office of the Commissioner for Personal Data Protection

https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page1j_en/page1j_en?opendocument; and

https://edpb.europa.eu/about-edpb/about-edpb/members_en.

The right to lodge a complaint with the relevant protection authority does not restrain the Parties to settle a dispute as per section 18 of this Privacy Notice.

14. Children Under 16

Our site is not directed toward children under 16 and we will not knowingly collect information for any child under the age of 16. If you are the parent of a child under the age of 16 and have a concern regarding your child's information on our site, please contact us at info@youhodler.com.

15. Services Located in the European Union

Our website and associated services are hosted within the European Union, EEA, Switzerland and the United Kingdom.

16. Data Protection Officer

You can directly reach the data protection officer at the following address: gdpr@naumard.com.

A Swiss representative for the purposes of article 14 of the nFADP shall be the appointed Swiss data protection officer for YouHodler SA, who can be contacted at the following address: legal@youhodler.com.

17. Changes to Privacy Notice

Our Privacy Notice may change from time to time. We will post any changes to the Privacy Notice on this page or on the Application and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of changes to the Privacy Notice).

18. Jurisdiction and Governing Law

This Privacy Notice and any questions relating thereto shall be governed by the laws of the Republic of Cyprus, to the exclusion of any rules of conflict resulting from private international law.

Any dispute relating to this Privacy Notice must exclusively be brought before the Limassol courts in Cyprus.

19. Contact

To ask questions or make comments on this Privacy Notice or to make a complaint about our compliance with applicable privacy laws, please contact us through:

a) our email address: support@youhodler.com ;or
b) our address: Arch Makariou III, 172, Melford Tower, 3027 Limassol, Cyprus;or
c) our data protection officer: gdpr@naumard.com.

We will acknowledge and investigate any complaint pursuant to this Privacy Notice.

Annex 1 - Cross Border Data Transfer Countries

EU member States	GDPR
United Kingdom	Adequacy decision
United States of America	Additional security and organizational measures
Switzerland	Adequacy decision

OTHER RECIPIENTS OF PERSONAL DATA FOR THE PURPOSE OF PROCESSING (SUBPROCESSORS)

AWS - Compliance Program; GDPR Centre; Supplementary Measures Addendum;	Ireland	Infrastructure Provider providing hosting services and storage	Essential data in order to operate services and build the contractual relationship	
Infomaniak SA	Switzerland	Infrastructure Provider providing hosting services and storage	Essential data in order to operate services and build the contractual relationship	
Atlassian	Netherlands; USA; Australia; UK	Infrastructure Provider; Customer service management	Essential data in order to operate services and build the contractual relationship	
Cloudflare.com		Infrastructure Provider;	ANONYMISED DATA	
SumSub Ltd.	Germany	KYC Provider, Data Validation, Document Check, Biometric processing, Fraud Detection	Essential data in order to operate services and build the contractual relationship; Data collected for Compliance purposes with AML Laws &/or the EU; Data collected for Compliance purposes with other applicable laws and regulations	
Intercom	Ireland	Customer Account Support and Communications	Essential data in order to operate services and build the contractual relationship; Data collected for marketing purposes	
Twilio	USA/EU/ Switzerland	Communications technology Provider	Essential data in order to operate services and build the contractual relationship	ONLY applicable if Users elect to use 9SMS for 2FA.
Sendgrid	USA/EU/ Switzerland	Communications technology Provider	Essential data in order to operate services and build the contractual relationship;	ONLY applicable if Users elect to

				use Email for 2FA.
Mixpanel	UK/Spain/ Singapore	Product Analytics	Essential data in order to operate services and build the contractual relationship; Data collected for marketing purposes	
Customer.io	USA	Communications technology Provider	Essential data in order to operate services and build the contractual relationship; Data collected for marketing purposes	
PandaDoc	USA	Digital Signature Platform	Essential data in order to operate services and build the contractual relationship; Data collected for Compliance purposes with AML Laws &/or the EU; Data collected for Compliance purposes with other applicable laws and regulations	
Docusign	France, UK, Italy, Germany, Netherlands, Spain	Digital Signature Platform	Essential data in order to operate services and build the contractual relationship; Data collected for Compliance purposes with the AML Laws &/or the EU; Data collected for Compliance purposes with other applicable laws and regulations	
Typeform	USA, Luxembourg	Form Management	Data collected for marketing purposes	
Affise	Cyprus	Affiliate Marketing Management Platform	Essential data in order to operate services and build the affiliate's contractual relationship; Data collected for marketing purposes	ONLY applicable if User is part of affiliate network
Google Inc	Ireland Belgium, Germany, Switzerland,UK	Infrastructure Provider providing hosting services and storage; Internal Communications	Essential data in order to operate services and build the contractual relationship	
Slack	USA	Internal Communications	Essential data in order to operate services and build the contractual relationship	
WEGLOT.COM		Used by YouHodler.com to store user's	ANONYMISED DATA	

		language, and auto load preferred language version of the website.		

Annex 2 - Standard Contractual Clauses for International Transfers

The standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, are herein incorporated by reference and made available at:

https://commission.europa.eu/system/files/2021-06/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf

The specification of the modules applicable are available in our Data Processing Addendum which is available upon request via email at: legal@youhodler.com.

Annex - 3 : Data Processing Addendum

A Data Processing Addendum defining principles and specifying the SCC modules applicable for the processing of Data throughout a contractual relationship and the technical and organizational security measures, is available upon request via email to the following: legal@youhodler.com.