Privacy Policy *www.coinmixed.eu*

1. **Objectives**

The objective of this Policy is to ensure that the data processing rules of the website **www.coinmixed.eu comply with the provisions of Mixed Trade Kft (2377 Örkény Fő u 20, VAT: HU24967170)** (hereinafter: Data Controller) comply with the pertinent statutory requirements and the rules of the trade with regards to data processing. The primary purpose of this policy is to ensure that the activities performed by Data Controller, i.e. the company handling the pertinent data, fully complies with Act CXII of 2011 on the Right of Informational Self-Determination (Information Act) and on Freedom of Information and the associated Act XLVII of 1997 on the Processing and Protection of Personal Data.

This Policy was drafted with the consideration of especially the following statutory obligations:

- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, 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, and repealing Directive 95/46/EC (General Data Protection Regulation), Act C of 2000 on Accounting (Accounting Act) and Act CVIII of 2001 on certain issues of electronic commerce services and information society services (E-Commerce Act);
- Act XLVIII of 2008 on Essential Conditions of and Certain Limitations to Business Advertising Activity (Advertisement Act)
- Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers
- Act CXXXVI of 2007 on Prevention and Combating of Money Laundering and Terrorist Financing
- Act CLV of 1997 on Consumer Protection
- Act CVIII of 2001 on certain issues of e- commerce services or services in connection with informational society;
- As an underlying statute, Act V of 2013 on the Civil Code (CC) applies.

This policy the also considers the rules laid down in the General Data Protection Regulation. Upon said regulation's entering into force, this Policy shall be reviewed. (https://www.naih.hu/files/Tajekoztato_adatved_nyilv_megsz.pdf)

1. **Scope of the Policy**

Based on the applicable provisions, Data Controller shall draft and implement a privacy policy. This Policy only covers data processing issues that fall within the scope of the statute. This Policy shall cover other data processing, direct marketing, any other commercial activities carried out by Data Controller or data processing of the website www.coinmixed.eu maintained by Data Controller. This Policy shall enter into force on 24 October 2018 and shall remain effective until further instructions. This Policy is applicable by Data Controller, data subjects of the processing under this Policy and individuals whose rights or legitimate interests are affected by such processing. Data Controller reserves the right to amend this Policy. Changes of this Policy may not cause infringements of data subjects' rights. Such amendments

may only be brought forth if adequately justified. Data Controller shall publish such amended Policies on its website.

1. **Definitions**
2. Data Subject: any defined, natural person identified or – directly or indirectly – identifiable using his/her personal data, who uses Data Controller's services, in other words register to the website eu;
3. Personal data: any information relating to the data subject, in particular names, identification numbers, one or more factors specific to the physical, physiological, mental, economic, cultural or social identities - or inferences with regards to the data subject that can be made from such data;
4. Consent of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the full or partial processing of personal data relating to him or her;
5. Objection: the data subject's statement wherein he/she objects to the processing of his/her personal data and requests cessation of such processing and/or erasure of his/her data subject to such processing.
6. Scope of Data: Identification data of natural persons: the purpose of the processing of such data is the unambiguous identification of the data subject. Data Controller will process the scope of identification data that is necessary and sufficient for the unambiguous identification of data subject.
7. Data Controller: natural or legal persons and/or organizations without a legal personality, who - independently or jointly with others - establishes the purpose of data processing, makes the decisions with regards to such processing (including the means of processing) and carries them out or causes them to be carried out by a data processor appointed by it.
8. data processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
9. Erasure: permanent destruction of data beyond recognition
10. Third parties: natural or legal person, public authority, agency or body other than the data subject, controller or processor;
11. third country: countries outside of the EEC
12. EEC permanent residents: Residents of European Economic Area (including The United Kingdom) or Switzerland (jointly „EEG residents"). Based on Article 6 of the GDPR or any equivalent regulation (Data Protection Act), we will process these personal data to comply with our legal obligations.
13. Confidential information: Data subjects' information handled by Data Controller shall constitute to confidential information

1. **Person and Activities of Data Controller**

Information of the Data Controller: Company name: Mixed Trade Kft. Registered seat: H-2377 Örkény, Fő utca 20. VAT ID: 249671-2-13 email: info@coinmixed.eu

1. **Principles of Data Processing**

Data Controller shall act in good faith and in compliance with the basic principles of fairness, in cooperation with data subjects. Data Controller shall exercise its rights and fulfil its responsibilities for the intended purposes only. During processing, personal data will remain such as long as the connection between the information and the data subject is restorable. The connection between the data and the data subject shall be deemed restorable as long as the Data Controller has the technical conditions necessary for such restoration. During processing, Data Controller shall ensure accuracy, completeness and – if regarding the purpose of the processing it is necessary – currency of the data and shall ensure that data subjects can only be identified until it is necessary for the purpose of the processing. By availing and using our services you accept the conditions of this Privacy Policy. If your consent is necessary to process your personal data, we will request collection, use and publication of personal data as follows. The Company may acquire further, „just-in-time" publications or further information with regards to the data collection, use or share of individual services. Such bulletins can clarify or complete the Company's data protection practices or adopt decisions of how the Company will process such data. If you don't agree or you are not conformed with this Privacy Policy, please cease availing/use of our services without delay. The Company uses Secure Socket Layer (SSL) coding technology to protect information provided to us. This technology serves prevention of circumvention of your information when you communicate with us. To adequately safeguard information, the Company's servers communicate with private networks through an industrial network, behind an industrial-quality hardware firewall. These data protection principles serve as guidelines for the Company's data processing to ensure full compliance of processing of your personal data with the statutory provisions. The Data Controller is responsible for the adherence to these principles. If necessary, lawfulness of its data processing has to be proven. Only information relating to natural persons shall be deemed personal data. Data Controller agrees to process data entrusted to it in compliance with the effective regulations and abides by the statutory data processing principles and the obligations of purpose limitation, minimization and security. Furthermore, Data Controller agrees to respect data subjects' right to informational self-determination, and - except if required by law - will not disclose personal data to third parties. Personal data may only be processed for pre-defined purposes, and to the extent and time period necessary for the given purpose. Processing of personal data shall be based on statutory authorizations or - if this is not the case - the data subject's free and informed, voluntary consent. According to the principle of fair processing, the data subject may never become a mere object of the process of personal data processing. Data subjects may not become helpless against the Data Controller or other persons with regards to the provision over his/her personal data. Data processed by adhering to the principle of data quality shall be accurate, complete and up-to-date, respective of the purpose of processing. Based on the security principle, data shall be protected by all reasonable measures allowed by the latest technologies against unauthorized access, alteration, unauthorized dissemination, damages or destruction. The fact, location, purpose of the processing, the person of the data controller

and the policy of such processing shall be public. Pursuant to the principle of personal participation, data subjects may view, amend, supplement and request erasure of his/her data as per the applicable statutory provisions. Principles of Data Processing and obligation of adherence to these are binding to both the Data Controller and the Data Subject.

1. **Purpose of processing**

Data Controller may process personal data exclusively for a defined purpose, for exercising rights or fulfilling obligations. Such processing shall correspond to the purpose of processing in every stage thereof. Collection and processing of data shall be fair and lawful. Data Controller puts forth all the efforts to confine the scope of processed personal data to data that are essential for the realization of the purpose of the processing. Personal data may only be processed to the extent and time period necessary for the given purpose, in compliance with the statutory requirements.

1. **Legal Basis of Data Processing**

Data Controller primarily bases processing of data subjects' personal data on their consent. Data subjects' contact of Data Controller and availing its services shall constitute to Data Subject's consent to the processing under this Policy. Consent includes all personal data provided by Data Subject to Data Controller. Consent also includes data that are generated in connection with Data Controller's activities. Certain data processing are required by law; these are mandatory. Data Controller shall primarily apply the mandatory rules of data processing set forth in the pertinent legislation. If a regulation is valid and effective, Data Controller shall act in compliance with it and may not question the practicality, professionality or constitutionality thereof. Data Controller is responsible for the identification of data subjects in order to comply with the applicable legislation when processing data. For this purpose, Data Subject voluntarily provides his/her data to Data Controller, who shall record such data.

1. **Method of Data Processing**

Data Controller shall collect data about its partners directly from data subjects. Data Controller my call Data Subject to verify the data provided by Data Subject. In such cases, Data Subject shall verify such data by presenting his/her documents. Data Controller may examine such documents to verify correctness of the data provided by Data Subject. Verification and registry of the affected partners is necessary to allow tracking of such data. The primary aim of collecting personal data is to be able to provide secure, smooth, efficient and customized services to you. Usually, we use personal data for the provision of our services, to create and develop, operate and transmit content and ads or prevent losses and combat fraud. This information are used as follows:

- Maintenance of legal compliance and adherence to rules.

Some of our basic services fall within the scope of legislation and regulations that are collecting and using your personal identification information, your official identification information, financial information, transaction details, employment information, online user name and/or user data. The Company shall identify and verify its clients in connection with the use of our services to comply with the regulations of combating money laundering and

financing of terrorism. Additionally, for the verification of your identity, we solicit the services of third parties. Such verification will be carried out by comparing the third party's databases and public registries with the personal data provided by you. If, in connection with your personal account, authorizations are necessary to raise purchase and sale limits, you will need to provide further information that will be used for the verification of your identity, address, digital currency or to determine whether you can manage the risk in cooperation with the service providers acting on our behalf, in compliance with the applicable law. However, if you do not provide your personal data, this will result in closing your account, because we are not able to provide our services in compliance with the statutory requirements and/or other rules.

- Enforcing our Services Agreement and other Agreements

Our Company processes sensitive information, for example your identification information and other financial data, therefore, active monitoring, analysis, prevention or mitigation of potentially prohibited activities is very important to us. This way we enforce our agreements with third parties and/or user agreements sent out, along with other agreements for various services. Additionally, we may need to charge fees, based on the use of our services. We collect information about account activities and we strictly monitor the connections with our services. We use your personal data collected through our services for the above purposes. Refusal of processing of your personal information for these purposes will result in closing down of your account, as this precludes our provision of the services in compliance with the applicable conditions.

- Provision of our Services

Your personal data will be processed to provide our services to you. For example, if you would like to buy digital currency, we will ask for certain information, for example a user name, contact details or payment information. Without this information, we cannot provide our services to you.

- Communication when Providing Services

We provide you with administrative information or information in connection with your account to keep you updated regarding our services, security problems, updates and/or other information regarding transactions. Without such communication, you may miss some important updates that may affect the way our services are used.

- Customer Service

If you contact us, we may be able to solve any arising issues, disputes, questioned fees or repair of bugs.

- Quality Assurance

Your personal data are processed to provide quality assurance and for the training of our staff to ensure continued provision of accurate information to you. If we don't process your personal data for the purposes of quality assurance, you may experience interruptions in the services, inaccurate transaction records or other problems. The basis of this processing is the

necessity of fulfilment of our contractual obligations. EEC permanent residents: Pursuant to the data protection regulation of the EEC, for all the above categories (except for point 1), the personal data will be processed by us under the Agreement we entered into.

- Network- and Information Security

To enhance security, to monitor and verify identities and/or access to our services, to combat spam or malware or security threats and to comply with the applicable security statutes and regulations, we will process your personal data. Threats to Internet are continuously developing, therefore, having accurate and up-to-date information about the use of our services is paramount. Without processing your personal data, we may not be able to guarantee security of our services. EEC permanent residents: In line with the EEC data protection regulation, we process these personal data to comply with statutory provisions.

- Research and Development Purposes

Your personal data will be processed to understand the way you use or contact the services offered by our Company. Furthermore, we use such information to customize, measure and repair our services, to develop the contents and layout of our website and/or new services. Without such processing, we may not be able to continuously provide our services. The basis of such processing shall be the legitimate interests of Parties. EEC residents: In line with the EEC data protection regulation, we process these personal data to comply with the above legitimate interest.

- Enhance the user experience of our website

Processing of your personal data will be carried out in a customized way, making the desired settings. For example, you can opt to provide access to personal data stored by third parties. In case this processing does not take place, we may not be able to continuously provide our services or part thereof. EEC residents: In line with the EEC data protection regulation, we process these personal data to comply with the above legitimate interest.

- Marketing Activities

Based on our communication preferences, we may send you marketing materials to inform you about own- or third-party events (targeted marketing) or promotion offers based on your communication preferences. To provide you with such marketing materials, we use information about your use of our services and your contact details. You may opt out of marketing communication any time. EEC residents: In line with the EEC data protection regulation, we process these personal data to comply with your consent.

- Photocopying of Your Documents

Documents containing personal data may be photocopied when you intend to subscribe to our services in person. In such cases, the photocopy shall be prepared in a way to only capture the essential data. The Data Controller shall be exhaustively familiar with the purpose of photocopying, which shall be subject to Client’s written consent.

- Use of Cameras and Recording of Phone Conversations

To ensure smooth operation and for the protection of life, people's physical integrity, personal freedom, security and trade secrets, our Company may take photos and video recordings in the room open for customer service. Such photos/recordings may be stored for security purposes or serve as an evidence. Pursuant to Act CXXXIII of 2005 on persons and property protection and on the activity of private detectives, such recordings may be retained for 60 days. The legal basis for the recording of phone conversations is not the voluntary consent of data subjects, but a statutory authorization: subsection (3) of section 17/B. of Act CLV of 1997 on Consumer Protection sets forth recording of telephone communication between customer services and consumers. In case you do not give your consent to the recording of the phone conversation you are a party to, you may not avail our customer services to otherwise automated services, either. Purpose of recording such telephone conversations: Protection of data subjects' and Data Controller and guarantee of provability after such conversations took place. When recording phone conversations, we store the following information: telephone number, date and time of the call, the voice recording captured of the conversation and the personal data provided during the conversation. We will retain such recordings for 5 years. The recordings will be made searchable by telephone number and date of the of the call. Upon request of the data subject, the recording will be released to Data Subject on a data storage device, as per the below procedure: Data Subject requests issuance of the recording to him/her, wherein Data Subject shall indicate the telephone number he/she placed the call from, his/her name and the date and time of the call (day, month and year as a minimum). Data Subject shall send a pen-drive along with the request and shall provide a password for coding of the recording and the address he/she intends to receive the recording to. The written your request shall be transmitted to the registered seat of our Company, and within 15 days, we verify the lawfulness of the release of the information. In case the information is lawfully releasable, our Company will send the requested information to the requestor by registered mail. In case we may not release the requested data, we will return the data storage device to the requestor in its original form, along with the justification of the rejection of his/her request. Your personal data will not be used without your permission for purposes other than you provided such data for. From time to time, we may request your permission to disclose your personal data to third parties. You may opt out of disclosing your personal data to third parties or of allowing us to use your personal data for purposes other than such data were collected for or purposes other than permitted by you later. Should you decide to restrict use of your personal data, certain services and/or services of the Company may no longer be available to you. Data Controller's website will collect general data and/or information when a person or an automated system visits the website. This information are stored in the log files of the server. The collected information may entail the following: (1) Browser types and versions used, (2) The operating system used by the access system, (3) The website where an access system accessed our website from (so-called references), (4) Sub-sites, (5) Date and time of accessing the website, (6) Internet protocol address (IP address), (7) The Internet service provider used by the access system, (8) any other similar data or information available to us if attacks against our IT system occur. During the use of such general data or information, Data Controller will not make any inferences about natural persons. We much rather need the following information: (1) for the provision of our products and services, including this website to improve them in time, (2) to provide a correct website content, (3) to optimize the content and the advertisement of our website, (4) to ensure the

long-term viability of our IT system and website technologies, (5) to customize and maintain our relations with our customers, for example offers products or services to customers that may be interesting for them. (6) to examine, react to or handle questions or events, and (7) to release information necessary for criminal procedures to law enforcement bodies if cyber attacks occur. Therefore, Data Controller statistically analyses anonymized data or information to enhance the Company's information security and ensure an optimal level of protection of personal data processed by us. The anonym data of the server log will be stored separately from any other data provided by the data subject.

1. **Confidentiality**

Data subjects' information handled by Data Controller shall be considered as confidential information. Confidential data shall be handled by Data Controller in compliance with the applicable regulations, with special regards to safeguarding confidentiality of such information. Confidential data shall be adequately protected by the Data Controller, as per the provisions of this Policy. We are aware of the importance of confidentiality; therefore, the Company maintains (and obliges its service providers to do the same) adequate physical, technical and administrative measures to protect your personal data and the confidentiality of such data. Personal- or transaction information or parts thereof – including certain confidential bank accounts and/or route numbers – may be stored or processed by us anywhere in the world where our facilities or service providers are located. Your personal data are secured by our adherence to the applicable regulations and rules and by maintaining physical, electronic and procedural guards. For example, we use computer-based guards, such as firewalls, data encoding, access control facilities and -files. We only allow access to personal data for staff whose access is necessary for the completion of their tasks. However, we cannot guarantee that loss, misuse, unauthorized access or alteration of data will not occur. Please, take your role in the protection of your personal data seriously. When you subscribe to our services, choosing a long and complex enough password is important. You should not disclose such passwords to third parties, and you should inform us of any unauthorized access to your account without delay. In addition, we cannot guarantee security or confidentiality of data sent or received through the Internet or wireless connections, for example e-mail, telephone or text messages, as we are not in the position to protect these until we receive those. Should you have a good reason to assume that your data are no longer secure, we request you to contact us at our e - mail address, mailing address or telephone number indicated below.

1. **Term of Data Processing**

Based on the statutory requirements, Data Controller shall process such data for 10 years. After 10 years, Data Controller shall delete or destruct such data. If statutory requirements exist to retain data for longer or shorter time periods, Data Controller shall process data for the time period set forth in the regulation.

1. **Transmission of Data**

Data transmission shall always be based on the data subject's written consent or a statutory authorization. Data Controller shall only transmit personal data if the legal basis for such transmission is clear, and the purpose and the person of the recipient is exactly defined. Data Controller shall always document such transmissions in a way to allow for the evidencing of

the process and lawfulness thereof. Such documentation can be based on duly issued documents requesting or setting forth of such data disclosure. Data transmissions required by law shall be carried out by Data Controller. In addition to the above, personal data shall only be transmitted if the data subject gave its consent for such transmissions. Data Controller shall ensure adequate logging of data transmissions to allow for the traceability of the recipient, method, date and time and the scope of the data of such transmissions.

1. **Handling of Files**

Data Controller shall ensure that the method of logging of such data corresponds to the requirements of the operational regulations. The principles and obligations under this Policy shall be adhered to in the cases of both paper-based and electronic records. Data Controller shall provide access to the data log in compliance with the requirements of data security for individuals involved in the identification and service of the data subject. Data Controller shall ensure that other persons do not access such data. Data Controller shall operate the electronic log by way of an electronic software meeting the requirements of data security. The software shall ensure that the data can only be accessed by individuals who need such access to fulfil their obligations, for the intended purposes and under controlled circumstances. If possible, Data Controller makes all reasonable efforts to comply with the principle of minimalizing access to cause individual employees and other persons acting on behalf of and for Data Controller to access only the personal data necessary for the completion of their tasks.

1. **Data Security**

Data Controller shall ensure the security of data. To realize this, Data Controller takes the necessary Technical and organizational measures regarding files stored both on IT devices and paper-based data storage. Data Controller shall ensure compliance with data security rules laid down in the pertinent legislation. Data Controller shall take all technical and organizational measures and implements procedural rules necessary to comply with the applicable regulations and data protection- and confidentiality rules. Data Controller shall put forth all efforts to protect the data against unauthorized access, alteration, transmission, disclosure, deletion, (inadvertent) destruction, damages or becoming inaccessible due to changes in the used technology. In establishing the measures serving data security, Data Controller shall take the development level of the latest technology available. Out of the several solution options, Data Controller shall choose the one providing the highest level of protection of personal data, except where this would impose a disproportionate burden on Data Controller.

1. **Data Processor**

Data Controller reserves the right to solicit the services of a data processor, by way of a permanent or case-by-case instruction. For the use of the services of a data processor, the applicable legislation, especially the provisions of the Information Act shall apply. Use of data processing services shall be strictly based on a written agreement. Upon request, Data Controller shall inform data subjects about the person of the data processor and about the details of its processing activities.

1. **Erasure, Archiving of Data, Handling of Data Unsuitable for Identification of Data Subjects**

Data Controller shall delete personal data, if

1. processing of such personal data is unlawful;
2. requested by the data subject (except for processing required by law);
3. the data are incomplete or erroneous, and this condition cannot be lawfully remedied – provided that deletion is not prohibited by law;
4. purpose of processing has ceased to exist, or the period of statutory retainment of such data has expired;
5. it is ordered by the Hungarian National Authority for Data Protection and Freedom of Information (NAIH).

Deletion of data processed upon on the data subject's voluntary consent may be requested by the data subject in certain cases. Instead of deletion, Data Controller shall block the personal data upon Data Subject's substantiated request, or, if based on the available information, it can be presumed that the Data Subject's legitimate interests are infringed. The personal data blocked this way can only be processed until the purpose of such processing that precludes deletion exits. Data Controller shall mark the personal data processed by it, if the Data Subject challenges the correctness or accuracy of such data, but incorrectness or inaccuracy of the personal data in question cannot be clearly established. For processing required by law, deletion of such data shall be subject to the provisions of the respective legislation. In case of deletions, Data Controller shall make such data unsuitable for identification of the Data Subject. If required by law, Data Controller shall destroy the data storage containing the personal data in question. Data Controller reserves the right to log deleted data in a way that is unsuitable for the identification of Data Subject.

1. **Rights of Data Subjects and Exercise of Such Rights**

Information: Data Controller shall inform Data Subject of processing of his/her data in advance. Such notification shall primarily be done by way of the data subject's statement of consent and this Policy. Upon request of the Data Subject, Data Controller shall disclose information about Data Subject's data processed by it or by a data processor acting on its behalf, the sources of such data, the purpose and legal basis of processing, the name, address of the data processor and its activities regarding the processing, and – if the Data Subject's personal data are transmitted – about the recipient and legal basis of such transmission. Data Controller shall provide the requested information in writing as soon as possible, but within 30 business days of receipt of the request the latest. Such information shall be provided free of charge, provided that the requestor hasn't applied for information regarding the same scope of data in the same calendar year. In cases specified by law, such requests may be denied.
Rectification: Data Subject may request rectification of his/her erroneous personal data.
Erasure: Except for processing required by law, the Data Subject may request erasure of his/her personal data. Data Controller shall inform Data Subject of erasure of his/her data.
Objection: Data subject may object against processing of his/her personal data as per the provisions of the Information Act.

Controller's Procedures: During the release of information, rectification, erasure, and objection, Data Controller shall act in compliance with the applicable regulations. Data Controller's denial of the request for information, rectification, blocking or erasure shall entitle Data Subject to bring the case on to the court or on to the Hungarian National Authority for Data Protection and Freedom of Information. Upon request, Data Controller shall inform Data Subject of the available redress options.

1. **Internal Data Protection Officer and Data Protection Records**

Data Controller's Data Protection Officer

1. shall ensure adherence to the data protection controls,
2. shall supervise data controllers' and data processors' processing activities,
3. shall initiate implementation of new technologies and tools developed in the field of information security and data protection.
4. shall provide training for staff involved in data processing,
5. for scientific researches, shall authorize access to medical documentation.

Decisions regarding other issues not falling within the scope of the Data Protection Officer's responsibilities arising during the processing of data, shall be made by the head of the Data Controller. Based on the applicable version of the Information Act, entering processing carried out by Data Controller in the data protection register maintained by the Hungarian National Authority for Data Protection and Freedom of Information is not required.

1. **Legal Redress**

Should you have questions, remarks or complaints regarding these data protection guidelines, please contact us at info@coinmixed.eu, our support page or at the following mailing address: **Mixed Trade Kft (2377 Örkény Fő u 20, VAT: HU24967170)** Complaints regarding data processing shall be addressed to the Hungarian National Authority for Data Protection and Freedom of Information: Address of the Hungarian National Authority for Data Protection and Freedom of Information (NAIH): H-1125 Budapest, Szilágyi Erzsébet fasor 22/c Mailing address: H-1530 Budapest, Pf. 5. Telephone number: +36 (1) 391-1400 Fax: +36 (1) 391-1410 Email: ugyfelszolgalat@naih.hu Website: www.naih.hu In data subjects disagree with Data. We reserve the right to change the content of this Policy at any time, insofar such changes are permitted by law. You can contact the Data Controller at: info@coinmixed.eu Should you have any questions with regards to the Company, your personal information or regarding these data protection guidelines, you may ask us at info@coinmixed.eu. This Privacy Policy shall enter into force on february 2021.