PRIVACY NOTICE

for the Clients of Tiwala Solutions Kft.

Tiwala Solutions Korlátolt Felelősségű Társaság (registered seat: 1131 Budapest, Mosoly utca 40/A, floor 1, door 3.;, company registration number: Cg.: 01-09-343101), as a data controller (**"Data Controller"** or **"Company"**) shall respect the personal rights of its customers and partners (**„Data Subject"**), in particular the data protection rights thereof set out in Regulation (EU) 2016/679 of the European Parliament and of the Council (**"GDPR"**), and Act CXII of 2011 on the Informational Self-Determination and Freedom of Information (**"Privacy Act"**), and shall obligatory apply these rules in all cases during the performance of its activities and shall consider them to be governing, together with the provisions of this document.

I. PRINCIPLES OF DATA PROCESSING

Personal data shall be

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**),
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**'purpose limitation'**); further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes,
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**),
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**'accuracy'**),
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (**'storage limitation'**),
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**'integrity and confidentiality'**).
7. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (**'accountability'**).

II. DATA CONTROLLER

Data of the Data Controller:

Name: **Tiwala Solutions Kft.**
Registered seat: 1131 Budapest, Mosoly utca 40/A, floor 1, door 3
Company registration number: 01-09-343101
Email: legal@coincash.eu

III. PURPOSE AND LEGAL BASIS OF DATA PROCESSING

The Data Controller shall process the personal data provided or made available in any way by the Data Subjects (including documents submitted by the Data Subject to the Data Controller, as well as in any other form) in accordance with the legislation on business secrets and data protection regulations, exclusively for the following purposes:

- Purchase of virtual currencies („Service"),
- Development, improvement of the Service, increasing the user experience,
- Activity related to the promotion; raising awareness and sale of the Service,
- Customer care activity, contacting,
- Delivery of direct inquiries and newsletters,
- Implementation of customer identification processes related to combating money laundering and terrorist financing in order to complete duties under Section 7-14/A, 15 and 16-17 of the Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing ("AML Act"),
- In order to prevent abuses and crimes, revealing the identity of customers for the purposes of the legitimate interests pursued by the Data Controller, as well as cooperating with the authorities in the detection of abuses and crimes,
- Protection of property.

The Data Controller may process the personal data of the Data Subject with a reference to the below legal basis:

i. consent by the Data Subject (Article 6(1) a) of GDPR),
ii. performance of a contract to which the Data Subject is a party (Article 6(1) b) of GDPR),
iii. in order to comply with a legal obligation to which the Data Controller is subject (Article 6(1) c) of GDPR, and
iv. for the purposes of the legitimate interests pursued by the Data Controller (Article 6 (1) f) of GDPR).

The Data Controller shall hereby inform the Data Subject that it has confirmed the necessity and proportionality of data processing by way of completing an interest balance test before a data processing for the purposes of its legitimate interest. The Data Controller shall provide the Data Subject with the results of the interest balance test upon a request thereby.

The below table shows each data processing purposes and the related legal basis:

Data processing purpose	**Legal basis of data processing**
Purchase and exchange of virtual currencies	Article 6 (1) a) of GDPR, and Article 6 (1) b) of GDPR
Development, improvement of the Service and increasing user experience	Article 6 (1) a) of GDPR,
Activity related to the promotion, raising awareness and sale of the Service	Article 6 (1) a) of GDPR,
Customer care activity, contacting	Article 6 (1) a) of GDPR,
Delivery of direct inquiries and newsletters	Article 6 (1) a) of GDPR,
Implementation of customer identification processes related to combating money laundering and terrorist financing	Article 6 (1) c) of GDPR (Section 7-14/A, 15, and 16-17 of the AML Act)
Revealing the identity of customers for the purposes of the legitimate interests pursued by the Data Controller for the prevention of abuses and crimes	Article 6 (1) f) of GDPR, and Article 6. (1) a) of GDPR,
Cooperating with the authorities in the detection of abuses and crimes	Article 6 (1) c) of GDPR
Protection pf property	Article 6 (1) f) of GDPR

IV. SCOPE AND SOURCE OF PROCESSED DATA

The Data Controller shall process the following personal data for the above purposes within the course of its activities:

(i) family and first name,
(ii) family and first name at birth,
(iii) mother's name,
(iv) place and date of birth,
(v) type and number of identification deed,
(vi) client number,
(vii) telephone number,
(viii) mobile number,
(ix) e-mail address,
(x) bank account number,
(xi) so called wallet-identifier,
(xii) user name,
(xiii) password,
(xiv) personal data on the proof of residence,
(xv) personal data on the deed provided with the purpose of verifying source of funds,
(xvi) data on the Politically Exposed Person status,
(xvii) vide recordings,
(xviii) photos,
(xix) voice recordings,
(xx) type of used browser,
(xxi) IP-address.

The Data Controller shall obtain the processed personal data directly from the Data Subject.

V. COOKIE POLICY

During visiting the Data Controller's websites, cookies may be placed in the computer of the Data Subject. Certain cookies are essential for the proper functioning of the website, other are collecting information about the user habits regarding the website in order to increase the user experience. Certain cookies may disappear by closing the browser, there are however such cookies as well which may be longer available on the computer.

The Data Controller shall use the following cookies on its website:

Session cookies:

Session cookies are necessary to browse the website and to use the functions that shall guarantee the proper functioning thereof. The validity period of these cookies shall extend to the duration of the given visit, they shall be automatically deleted at the end of the session or when the browser is closed.

Proper session on the website shall be ensured upon the authorization provided in Section 13/A (3) of Act CVIII of 2001 on certain issues of electronic commercial services and services related to the information society, in accordance with the provisions therein.

The website shall use the following session cookies:

- JSESSIONID: technical cookie applying session identifier.

  This cookie shall help the content management system to manage the user pageviews as a continuous session in order to ensure that certain basic functions, such as

registration and login, can work flawlessly. They shall be deleted from the visitor's computer by closing the browser window.

Preference cookies

With the help of these cookies, the website shall remember the mode of operation chosen by the Data Subject (e.g. language selection). This shall be done so that you do not have to enter them again on your next visit.

The following are the cookies that shall support the use of the website:

- COOKIE_SUPPORT: „cookie support testing cookie"

  This cookie shall help the content management system used on our site to detect if a user has disabled the use of cookies. It is valid for 2 years from the date of visit.

Analytical cookies:

With the help of analytical cookies, the Data Controller shall collect information about the Data Subject's website user habits in order to develop the website accordingly.

The website uses the following cookies for the anonymous analyse of the user activity:

- Certain functions of Google Analytics

  One functions thereof shall support the anonymous detection whether a user has visited the website before. It is valid for 2 years from the date of visit.

  An additional function shall prevent the system that collects anonymous statistics from receiving too much data in a short time. It is valid for 1 minute after the visit.

  Detailed information about the service is available via the following link: https://www.google.com/analytics/terms/us.html

Tracking cookies

In case of certain tracking cookies, it is possible that the cookie may forward not only anonym information on the Data Subject, provided that we shall use technical tools and measures in order to avoid that personal data are getting known (for example data masking), and we shall continue to use the information obtained to have an anonym analyse of the user habits.

The website uses the following tracking cookies:

- Smartlook

  A service used for heat map analysis, which collects information about the location of clicks and the movement of the mouse. We use it anonymously to check how well users can actually use the website. The application thereof makes it possible for us to develop our content in such a way that visitor can get in touch with our services easier and in an even more understandable way. They are deleted from the visitor's computer by closing the browser window.

  Detailed information (available only in English):

  https://www.smartlook.com/help/privacy-statement/

Targeted advertising cookkies

Application of these cookies is two-folded: they ensure the display of advertisements on third party website which the Data Subject is interested in or which are stored by the Data Controller. These cookies generally record the visits of websites, visits to certain product pages, forms and thank you pages, the duration of the visit and the device used.

The website is using the following targeting and advertising cookies:

- Google Adwords

  Detailed information on the service is available via the following link: https://www.google.com/intl/hu/policies/privacy

Check and disabling of cookies

Detailed information on cookie settings of certain browsers is available via the following link:

- Google Chrome
- Firefox
- Microsoft Internet Explorer 11
- Microsoft Internet Explorer 10
- Microsoft Internet Explorer 9
- Microsoft Internet Explorer 8
- Safari

VI. DURATION OF DATA PROCESSING

The Data Controller shall process personal data until the fulfilment of the purpose of data processing. In exceptional cases, in the event of complying with statutory obligation, the Data Controller shall process the personal data of the Data Subjects even after the termination of the legal relationship.

VI. DATA PROCESSING

The Data Controller shall hereby inform the Data Subjects that it is applying the following data processors during the provision of the Service:

- Zendesk (operation of customer care system) www.zendesk.com
- Zendesk Chat (Zopim) (operation of live chat system) www.zendesk.com
- SEON.io (application of security risk assessment service) www.seon.io
- Cloudflare (application of cyber security service) www.cloudflare.com
- Smartlook (marketing tool, a service aiming at increasing the user experience) www.smartlook.com
- Amazon Web Services (server service) https://aws.amazon.com/
- Slack (értesítések) www.slack.com
- Onfido KYC solutions - https://onfido.com/

VII. DATA TRANSFER

The Data Controller has a statutory obligation to provide data to the court, the prosecutor, the administrative authority, the public authority, the investigative authority, or other bodies in order to provide information, provide and transfer data, or make documents available. In this context, the provision of data shall only be to the extent that is absolutely necessary to achieve the purpose of the authority requiring the data provision - if the authority has specified the

exact scope of data and the exact purpose. The Data Controller shall not be held liable for the performance of this type of data transfer, as well as for the possible resulting consequences, and submission of claims against it shall not be possible.

VIII. DATA SUBJECT'S RIGHTS

1. Right to transparent information and communication

   The Data Controller shall take appropriate measures in order to provide the Data Subject with all information and notification regarding the processing of personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing.

2. Right to information on and access to personal data

   The Data Controller shall provide the Data Subject with the following information at the time of obtaining the personal data:
   - specification of the Data Controller and the representative thereof, as well as his / her contact details,
   - purpose of the planned data processing and the legal basis thereof,
   - specification of the person or organization concerned with the data transfer,
   - the period for which the personal data will be stored,
   - the right to request from the Data Controller access to and rectification or erasure of personal data or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability,
   - the right to lodge a complaint with a supervisory authority,
   - right to withdraw consent at any time
   - whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

3. Data Subject's right to access

   The Data Subject shall have the right to obtain from the Data Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the given information.

4. Right to rectification

   The Data Subject shall have the right to obtain from the Data Controller without delay the rectification of inaccurate personal data concerning him or her, as well as to request the adjustment of the incomplete personal data.

5. Right to erasure, to be forgotten

   The Data Subject shall have the right to obtain from the Data Controller the erasure of personal data concerning him or her without undue delay where one of the following grounds applies
   - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,
   - the Data Subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing,
   - the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing,
   - the personal data have been unlawfully processed,

- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Data Controller is subject
- the personal data have been collected in relation to the offer of information society services

The Data Controller shall hereby inform the Data Subjects that it shall not be obliged to fulfil the request to exercise the right to erasure or to be forgotten to the extent that the data processing is necessary:

- for exercising the right of freedom of expression and information,
- for compliance with a legal obligation requiring data processing or for the performance of a task carried out in the public interest;
- for reasons of public interest in the area of public health,
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- for the establishment, exercise or defence of legal claims

6. Right to restriction of processing

The Data Subject shall have the right to obtain from the Data Controller restriction of processing where one of the following applies:
- the accuracy of the personal data is contested by the Data Subject, for a period enabling the Data Controller to verify the accuracy of the personal data,
- the processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of their use instead,
- the Data Controller no longer needs the personal data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims,
- the Data Subject has objected to processing pending the verification whether the legitimate grounds of the Data Controller override those of the Data Subject.

7. Right to data portability

The Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a Data Controller, in a structured, commonly used and machine-readable format and shall also have the right to transmit those data to another controller without hindrance from the Data Controller to which the personal data have been provided, where:
- the processing is based on consent; and
- the processing is carried out by automated means.

In exercising his or her right to data portability, the Data Subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible

8. Right to object

The Data Subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, including profiling based on those provisions. The Data Controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which shall override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claim.

9. Automated individual decision-making, including profiling

The Data Subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

IX. Restrictions

Union or Member State law to which the Data Controller or processor is subject may restrict the scope of the rights provided for in paragraph VII, if such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure to safeguard:

- national security,
- defence,
- public security,
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security,
- other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security,
- the protection of judicial independence and judicial proceedings,
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions,
- a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority, and
- the protection of the Data Subject or the rights and freedoms of others,
- the enforcement of civil law claims.

X. Remedies

If a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed may occur ("Personal Data Breach"), the Data Controller shall undertake to report that without undue delay and, where feasible, within 72 hours the latest upon gaining knowledge thereabout to the National Authority for Data Protection and Freedom of Information (address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.; telephone: +36-1-391-1400; e-mail: ugyfelszolgalat@naih.hu; webpage: www.naih.hu) as supervisory authority with competence, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

If that Personal Data Breach is likely to result in a high risk to the rights and freedoms of the natural person, the Data Controller should notify the Data Subject about the Personal Data Breach without undue delay using clean and pain language to describe the nature of the Personal Data Breach.

The Data Controller shall hereby inform the Data Subject that he / she shall be entitled to lodge a complaint with the NAIH or to apply an application to the court in case of an infringement of his / her data protection rights. The Data Subject shall also be entitled to initiate proceedings before the court of appeal having competence based on his / her place of residence or stay.

If the Data Controller shall cause damage to others by unlawful processing of the Data Subject's data or by infringing the requirements of data security, it shall be obliged to compensate them, and if the Data Subject's right to privacy may be infringed by this behaviour, the Data Subject shall be entitled for compensation. The Data Controller shall be released from responsibility for the damage caused and from the obligation to pay compensation if it may

prove that the damage or the infringement of the privacy rights of the Data Subject was caused by a force majeure cause outside the scope of data protection.

The Data Subject may apply for legal remedies to the following authorities:

National Authority for Data Protection and Freedom of Information (address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.; telephone: +36-1-391-1400; e-mail: ugyfelszolgalat@naih.hu; webpage: www.naih.hu).

The Data Subject shall be entitled to seek remedy by court in case of an infringement of its rights.

XII. DATA SECURITY

The Data Controller shall implement* appropriate technical and organizational measures, taking into account the state of science and technology and the costs of implementation, as well as the nature, scope, circumstances and purposes of data processing and the variable probability and severity of the risk to the rights and freedoms of natural persons, in order to guarantee a level of data security appropriate to the risk level, including:

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

1 May, 2022, Budapest

Tiwala Solutions Kft.