

PRIVACY POLICY

1. Validity and use of privacy policy

This Privacy policy (hereinafter: the Policy) shall apply to anybody who is, in accordance with the General conditions of the Coinpennant.com_web portal, considered a user, and for the entire web portal, all its components and sub-sites.

This Policy applies when a user visits the web portal for the first time and in all subsequent visits. By using the web portal the user confirms that he accepts and agrees with all the provisions of this Policy.

This Policy may be amended or supplemented without warning or notice. By using the web portal after the amendment of this Policy, the user shall confirm that he agrees with the amendments.

2. On personal data protection

2.1. Data controller

Personal data controller, collected in the use of the Coinpennant.com web portal, shall be CoinPennant d.o.o. (hereinafter: the controller).

2.2. Collected data on users

The controller shall collect the following data on users:

- for registered users:

(*)¹ e-mail

The user may communicate optional personal data if he so wishes. The user, who does not communicate optional personal data, shall not suffer any prejudicial effects for that.

The controller shall process also IP addresses of devices through which the users access to the web portal. The controller shall use cookies on the web portal, with which it identifies only the users, who use the function „Stay signed-in“, however, users identification is not possible this way.

¹ The indication of data marked with an (*) is obligatory.

2.3. Purpose of data processing

The controller shall use the collected data on users exclusively for the following purposes:

- keeping records of registered users,
- keeping records of Coinpennant.com project supporters,
- keeping records of subscribers to the news of the Coinpennant.com project,
- communication on development of the ICO Coinpennant.com project,
- information on the receipt of a token, its value and possible future payout of a token,
- keeping statistics and user analysis,
- classification of clients,
- compliance with legislation,
- keeping and processing of data under the ZPPDFT-1 (if it emerges in the future that we are liable for the payment of VAT),
- information on other interesting projects with ICO financing or other projects which Coinpennant d.o.o. considers interesting,
- information on current development in the crypto world and other purposes, important for relevant implementation of business
- and other processes of Coinpennant d.o.o. for the provision of better services.

2.4. Transmission of data

The controller shall transmit the collected data only to possible contractual processors and shall not transmit the collected data to any third person, except by virtue of the applicable legislation.

3. Data protection and data retention period

The controller shall safeguard personal data in accordance with this Policy and requirements for the personal data protection, provided by the Slovenian legislation and the EU regulations.

Personal data shall be kept only until the purpose of their keeping is fulfilled (storage period). Following the expiry of the storage period the personal data shall be deleted, destroyed, blocked or anonymised, unless the law or another regulation for individual types of personal data provides otherwise.

To delete personal data in electronic form, such a deletion method is used that reconstruction of all or any part of the deleted data is no longer possible.

4. Users' rights

A data subject shall have the right to revoke at all times the given consent for the processing of his personal data.

A data subject shall have the right to receive from the controller a confirmation, whether personal data related to him is processed, and if so, he shall have the right to access personal data and certain information.

A data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data in connection with him. A data subject shall have the right, taking into consideration the purpose of data processing, to supplement incomplete personal data, including submitting an additional declaration.

A data subject shall have the right to obtain from the controller deletion without delay of personal data in connection with him, and the controller shall delete such personal information without undue delay, when one of the following conditions apply:

- a) personal data are no longer needed for the purposes, for which they were collected, or in any other way processed;
- b) data subject revokes his consent on the basis of which the processing is made and for the processing of which no other legal basis exists;
- c) data subject objects the processing and no overriding legitimate reasons exist for their processing;
- d) personal data was processed unlawfully;
- e) personal data shall be deleted to comply with the legal obligations under the Union law or the law of the Member State to which the controller is subject;
- f) personal data has been collected in relation to the offer of the information society services.

A data subject shall have the right to obtain from the controller the limitation of processing, when one of the following applies:

- a) a data subject contests the accuracy of data, namely for the period, which enables the controller to verify the accuracy of personal data;
- b) the processing is unlawful and a data subject opposes the deletion of personal data and instead requires limitation of its use;
- c) the controller no longer needs the data for the purpose of processing, but a data subject needs it for the establishment, exercise or defence of legal claims;

- d) a data subject submitted an objection in relation to processing until it is verified whether legitimate reasons of the controller outweigh the reasons of a data subject.

A data subject shall have the right to receive personal data related to him, which were forwarded to a controller in a structural, generally used and machine readable form, and shall have the right to forward such data to another controller, without hindrance from the controller, which was provided the personal data.

5. Action in case of unauthorised access

In any suspicion of violation of personal data protection, the controller shall communicate such violation to the national personal data protection authority and in the event of suspected criminal offence to the police or prosecutors. Where it is likely that the violation of personal data protection may cause major risk for the rights and freedoms of individuals, the controller shall, without undue delay inform the data subject that a breach of personal data protection has occurred.

A data subject has the right to lodge a complaint with a supervisory authority, in particular with a Member State of residence, his place of work or where the breach has occurred, if he believes that processing of personal data related to him breaches the personal data protection regulations.

Where it is likely that the violation of personal data protection may cause major risk for the rights and freedoms of individuals, the controller shall, without undue delay inform the data subject that a breach of personal data protection has occurred.

6. Exclusion of liability

The controller shall not be liable for the damage resulting to the user from the fact that in registration the user transmitted to the controller erroneous, incomplete or inaccurate data.

7. Final provisions

Invalidity of any of the provisions of this policy, irrespective of the reason for their invalidity, shall not render the invalidity of the policy as a whole. In such case the invalid provision shall be considered as unwritten, and this Policy shall continue to apply without such a provision.

For legal relationship between the users and controllers the Slovene law and law of the European Communities shall apply (including the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 with regard to protection of individuals in

personal data processing and free movement of such data). Any possible disputes shall be resolved by a court at the place of the registered address of the controller, having jurisdiction as to the substance of the case.

In force from 1st November 2017.