

## Privacy Policy

15<sup>th</sup> August 2018

Please read this privacy policy ("**Privacy Policy**") carefully before participating in the ICO. This Privacy Policy forms part of the Accompanying Documents, governing the processing of personal data of the Users by the Company for the purposes of the ICO, for participating in the ICO and the usage of the website <http://vera.jobs> ("**Website**"). Please note that the Privacy Policy does not apply to the Services offered by the Company nor for registering an Account.

Capitalized terms in this Privacy Policy are used in the meaning given to them in the Terms unless otherwise expressly set out herein.

In case you are providing to the Company or Stafory personal data of third persons, you are obliged to provide to those persons the necessary notifications and, if required, make sure they acquaint themselves with the content of this Privacy Policy, as required under applicable legislation.

### 1 CONTROLLER

1.1 The personal data of the User processed for the purposes of the ICO has two joint data controllers:

1.1.1 ROBOTVERA OÜ. An Estonian limited liability company, with a registry code 1432721, registered address Narva mnt 36, Tallinn, 10152, Estonia. E-mail: [eu@robotvera.com](mailto:eu@robotvera.com);

1.1.2 OOO Stafory. A Russian limited liability company, with a registry code 1157847117592, registered address Ryleeva 6A, office 1-N, Saint Petersburg 191123, Russian Federation. E-mail: [info@robotvera.com](mailto:info@robotvera.com).

1.2 ROBOTVERA OÜ and OOO Stafory will be referred together as the "**Controller**". The User has the right to contact ROBOTVERA OÜ or OOO Stafory in respect of any User's personal data processing operations. References to "we", "us" and "our" mean references to the Controller.

1.3 ROBOTVERA OÜ and OOO Stafory have allocated between themselves the roles and responsibilities regarding the processing of personal data of the User as follows:

1.3.1 ROBOTVERA OÜ is responsible for the issuing of the VERACoin tokens and all the processing that relates to the know-your-customer obligations and the adherence of the foregoing to the applicable data protection regimes;

1.3.2 OOO Stafory is responsible for the maintenance of the Website, Platform and for the technical administration of the ICO.

The User, when participating in the ICO, makes available his/her personal data for the Controller, meaning, ROBOTVERA OÜ and OOO Stafory jointly and at the same time.

### 2 DATA PROTECTION OFFICER

2.1 The Users shall have the right to communicate with the Controller's data protection officer in order to obtain information on the processing of his/her personal data, using the following contact information:

E-mail: [olesya@robotvera.com](mailto:olesya@robotvera.com)

### 3 CATEGORIES AND SOURCES OF PERSONAL DATA THE CONTROLLER COLLECTS AND PROCESSES

**3.1** Personal data are information that can be used to directly or indirectly uniquely identify, contact, or locate a User as a private individual ("**Personal Data**"). The source of collected Personal Data depends on how the User communicates with the Controller.

**3.2** The Controller collects and processes the following categories of User's Personal Data:

**3.2.1 Wallet Data.** Including but not limited to: User's personal crypto currency account addresses ("**Wallet Data**").

Source: Provided by the User himself/herself.

**3.2.2 Know Your Customer Data.** The Controller may collect any data given related to participating in the ICO, including but not limited to: User's first and last name, personal identification code (if exists), date and place of birth, phone number and area code, e-mail, place of residence (address), profession or field of activity, whether or not the User is a politically exposed person ("**PEP**"), family member of PEP or person known to be close associated with PEP, data regarding beneficial ownership, copy of identification document, utility bill (for rent, electricity, gas, water, telecommunication services or other similar services), bank or credit card statement, tax bill, credit card type, expiration date, and certain digits of the User's card number, details of the User's transaction history. In case the User is a legal person, the following data may be collected and processed regarding the User's representative, including but not limited to: first and last name, basis for representation, data regarding beneficial ownership, copy of identification document, utility bill (for rent, electricity, gas, water, telecommunication services or other similar services), bank or credit card statement, tax bill. The following data may be collected and processed regarding the beneficial owner, including but not limited to: name, personal identification code (if exists), date and place of birth, place of residence ("**KYC Data**").

Source: Questionnaire filled out or data provided via other means by the User.

**3.2.3 Communication Data.** The Controller may collect any data relating to any correspondence exchanged between the User and the Controller, including any personal information retained in such correspondence, including but not limited to: User's name, e-mail, contents of the message, nicknames and/or social media account names and addresses, when contacting the Company via its official social media accounts ("**Communications Data**").

Source: Information the User provides during the communications.

**3.2.4 Technical Data.** The Controller may collect any device or ICO related information, that has been given and/or sent by the User, or by his/her device, to the Controller via using the Website or via other means of communication, including but not limited to: hardware model, operating system version, web browser used, unique device identifiers, statistics about the User's device, server log information (the date and time of visit, pages viewed, time spent on the Website, etc.) ("**Technical Data**").

Source: While the User uses the Website, the Controller collects Technical Data from the User's device automatically.

**3.2.5 Cookie Data.** The Controller uses cookies on the Website, which may collect User's Personal Data. For further information see Section 4 of this Privacy Policy ("**Cookie Data**").

## **4 COOKIES**

**4.1** The Controller is using cookies and similar technologies on the Website to analyse user-generated traffic, as well as enhance and optimize the user experience offered by the Website. To the extent allowed by User's browser settings and User's device, the User may consent the

use of third party cookies that track User' behaviour and show advertisements based on User's interests and preferences.

**4.2** The legal basis for using essential cookies is the Controller's legitimate interest to provide the basic functionality of the Website. The essential cookies include but are not limited to the following types of cookies:

4.2.1 Session cookies to maintain the functionality of the Website;

4.2.2 User-centric security cookies to detect authentication abuses;

4.2.3 Multimedia content player cookies to store technical data to play back video or audio content on the Website;

4.2.4 Load-balancing cookies for improving distribution of workloads;

4.2.5 User interface customisation cookies for determining language or font preferences.

**4.3** Data collected via cookies mentioned in Section 4.2 above are retained for a period of 30 days.

**4.4** The legal basis for using following cookies is User's consent. These cookies are applied or may be applied on the Webpage only after the User has given his/her consent for the application of such cookies:

4.4.1 Performance cookies and analytics technologies to collect information about how Users use the Website. The data collected via foregoing cookies are retained for 30 days.

4.4.2 Web beacons are bits of data that count the number of Users who access the Website and allow the Controller to see if a cookie has been activated. The Controller may use this information to identify which emails are more interesting to the Users. This information is aggregated and does not identify the User individually. The data collected via foregoing cookies are retained for 30 days.

4.4.3 Third party cookies applied by the Controller, but the application of which may result in revealing personal data related to the User to third parties and may result in storage or access to information stored on the User's terminal equipment:

4.4.3.1 Cookies deployed by vk.com are used for applying advertisements and retargeting it. The data collected via foregoing cookies are retained for 30 days;

4.4.3.2 Cookies deployed by yandex.ru and mc.yandex.ru are used for collecting the Website's visit parameters (time, page, source) and the User's parameters. The data collected via foregoing cookies are retained for 30 days;

4.4.3.3 Cookies deployed by youtube.com are used are used for registering anonymous statistical data on for example how many times the video displayed and what settings are used for playback. The data collected via foregoing cookies are retained for 90 days;

4.4.3.4 Cookies deployed by doubleclick.net are used for behavioural targeting, ad delivery and improved reporting on campaign performance. The data collected via foregoing cookies are retained for 90 days.

**4.5** The User has the possibility to allow or deny cookies using the browser settings. If the User prefers not to receive cookies, he/she may set the browser to refuse all cookies or send an alert when a cookie is issued. Additional information how to manage the cookie settings of the browser can be found here: [Internet Explorer](#), [Chrome](#), [Firefox](#), [Safari](#), [Opera](#).

## 5 THE PURPOSES OF AND LEGAL BASIS FOR PROCESSING PERSONAL DATA

**5.1** The Controller's legal basis to process User's Personal Data depends on the objective and context in which the Controller collects the Personal Data. The Controller processes Personal Data on the following four legal grounds: **performance of a legal obligation, performance of a contract, the Controller's legitimate interest** and User's **consent**.

**5.2** If the legal basis for processing User's Personal Data is:

5.2.1 legitimate interest, this means first and foremost the objective of improving the Website and carrying out the ICO;

5.2.2 consent, this means first and foremost the objective of ensuring an effective User experience by adjusting content, as without User's consent it would not be possible to tailor the Website to meet User's preferences;

5.2.3 performance of a contract, this means first and foremost the objective of preparing and fulfilling the token sales and purchase agreement in the form of the Terms;

5.2.4 compliance with an obligation arising from legislation, this means first and foremost that the Controller is required to process certain personal data by law. In this case the Controller cannot decide which data are collected, as it derives from applicable laws.

**5.3** The following depicts non-exhaustive list of processing purposes that are linked to specific data categories and legal basis for processing:

Processing purpose	Legal basis for the processing purpose	Categories of personal data used by the Controller for the processing purpose
Diagnose and repair problems with the ICO and the Website	Legitimate interest in providing data security and prevent fraudulent actions	Technical data
Administer the ICO, through the conclusion (including preparatory measures), enforcement of the Terms	Performance of the contract	KYC Data, Technical Data, Wallet Data
Enabling communication between the User and the Controller	Legitimate interest in carrying out the ICO	Communication Data, Technical Data
Providing the User a possibility to buy/sell VERACoin tokens from/to the Controller according to the Terms	Performance of the contract	KYC Data, Technical Data, Wallet Data
Providing functioning and accessible Website	Legitimate interest in providing basic functionalities of the Website with relevant	Technical Data, Cookie Data

	information about the ICO	
Performance of the KYC procedures	Legitimate interest in detecting and preventing crime, fraudulent actions with the purpose of monetizing the ICO proceeds	KYC Data
Improve, personalise and develop the Website	Legitimate interest in developing and enhancing the Website and the user experience in the course of regular business activities	Technical Data, Cookie Data
Verifying the User's identity	Performance of the contract	KYC Data
Tailoring the contents of the Website and general communication to suit User's preferences	Consent	Technical Data, Cookie Data

- 5.4** The Controller may process User's data for other purposes, provided that the Controller discloses the purposes and use to the User at the relevant time, and that the User either consents to the proposed use of the Personal Data or the new purpose is compatible with the original purpose brought out herein.

## **6 RETENTION OF PERSONAL DATA**

- 6.1** User's data (all categories mentioned in Section 3, except for Cookie Data) shall be stored for 10 years as of collection of such data, unless stipulated otherwise in applicable laws or down below.

6.1.1 Technical Data is retained for 5 years as of the collection of the Personal Data.

6.1.2 Wallet Data is retained for 5 years as of the collection of the Personal Data.

- 6.2** After the term mentioned in Section 6.1. of this Privacy Policy, the Controller will delete User's respective data immediately, except as noted below:

6.2.1 The Controller retains User's Personal Data for a longer period if it is necessary to comply with the Controller's legal obligations, meet regulatory requirements, resolve disputes, and enforce the Terms.

6.2.2 The Controller may anonymize the User's Personal Data and retain this anonymized information indefinitely.

## **7 SHARING THE PERSONAL DATA AND DATA TRANSFER OUTSIDE OF THE EU OR EEA ("EU/EEA")**

**7.1** Only the Controller's authorised processors have access to the personal data and they may access the data only for the purpose of conducting the ICO, resolving issues associated with the ICO and the Website.

**7.2** The Controller does not disclose any User-related data to any third parties except for:

Categories of Recipients	Reason for sharing
Law enforcement and data protection authorities	Only if the Controller is under a duty to disclose or share the User's personal data in order to comply with any legal obligation (for example, if required to do so under applicable law, by a court order or for the purposes of prevention of fraud or other crime).
Operational service providers (legal advisors, auditors etc. bound to confidentiality)	Ensuring adequate performance of the ICO and functioning of the Website; enforcing the Terms and other legal rights deriving from the Accompanying Documents.

**7.3** In addition to the third parties brought out in Section 7.2. of the Privacy Policy, the Controller may transfer personal data to third party service providers who act as processors and may operate the technical infrastructure that the Controller needs to host, store manage and maintain the Website, its contents and the data that Controller processes, also to provide data backup and security. The following depicts a list of authorised processors, their location and their reason for processing:

Authorised Processor	Processing purpose	Location	Website
Cloudflare Inc.	Protection against and mitigation of DDos attacks	USA	<a href="https://www.cloudflare.com/">https://www.cloudflare.com/</a>
SendPulse Inc.	E-mail service provider	USA	<a href="https://sendpulse.com/">https://sendpulse.com/</a>
Selectel Ltd.	Web hosting	Russia	<a href="https://selectel.ru/">https://selectel.ru/</a>
Functional Software Inc. (Sentry)	Real time error tracking	USA	<a href="https://sentry.io/">https://sentry.io/</a>

**7.4** The Personal Data the User provides to the Controller is made available to the Controllers (see Section 1.1. of this Privacy Policy) simultaneously. The key operational servers are under the control of OOO Stafory and are located inside the EU/EEA. Any further processing may involve data transfers to EU/EEA and to third countries.

**7.5** Please note that, some operational service providers might be located outside the EU/EEA, we may transfer the User's Personal Data outside the EU/EEA. In such cases the Controller shall opt to use special Personal Data protection safeguards, in order to ensure the safety of the User's Personal Data. The User has the right to get acquainted with or obtain information on the transferring of his or her Personal Data outside the EU/EEA by contacting the Controller using the contact information specified in Sections 1 and 2 of this Privacy Policy.

## **8 USER'S RIGHTS**

**8.1** If the User is a resident of the European Union or the European Economic Area, then the User has the following data protection rights, which can be exercised by contacting the Controller via contact information referred to in Sections 1 and 2 of this Privacy Policy. The User has the right to:

- 8.1.1 access his or her Personal Data processed by the Controller and may demand the correction of inaccurate personal data or demand the erasure thereof;
- 8.1.2 request restriction of the processing of the Personal Data in respect of them, or the right to object to the processing if it is based on the Controller's legitimate interest, as well as the right to portability of the User's Personal Data (transmission of the Personal Data to another legal or natural person), including by electronic means;
- 8.1.3 the User has the right of recourse to the Data Protection Inspectorate or a court if the User finds that his or her rights are violated in the processing of Personal Data, unless a different procedure for contestation is provided under applicable legislation;
- 8.1.4 not be subject to a decision based solely on automated decision making, including profiling, where the decision would have a legal effect on the User or produce significant effect.
- 8.1.5 withdraw his/her consent to the processing of Personal Data in the cases where the legal basis for Personal Data processing is the User's consent. For withdrawing the consent, the User may use the contact information referred to in Sections 1 and 2 of this Privacy Policy.

## **9 OTHER**

**9.1** The Controller may unilaterally modify the Privacy Policy from time to time. The latest version of the Privacy Policy is always accessible on the Website.

**9.2** This Privacy Policy also applies for the Users who have bought VERACoin tokens during the First Pre-Sale.

If the User has any questions regarding the processing of his or her personal data or exercising his or her rights in relation to the Privacy Policy please contact the Controller at the contact details provided in Sections 1 and 2 of this Privacy Policy.