

PRIVACY POLICY

We at Care.Wallet are committed to protecting your privacy. We have prepared this Privacy Policy to describe to you our practices regarding the personal data we collect from users of our website.

By using the Services, users consent to the collection and use of their Personal Data by us. You also represent to us that you have any and all authorizations necessary to use these Services including using them to process Personal Data. We collect and use the information you provide to us, including information obtained from your use of the Services. Also, we may use the information that we collect for our internal purposes to develop, tune, enhance, and improve our Services consistent with this Privacy Policy.

This privacy policy has been compiled to better serve those who are concerned with how their 'Personal Data' is being used online. Personal Information means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Please read our privacy policy carefully to get a clear understanding of how our website collects, uses, protects or otherwise handles users' Personal Data.

This Privacy Policy is intended to inform users about how our website treats Personal Data that it processes about users. If users do not agree to any part of this Privacy Policy, then we cannot provide its Services to users and users should stop accessing our services.

By using the Services, You acknowledge, consent and agree that we may collect, process, and use the information that you provide to us and that such information shall only be used by us or third parties acting under our direction, pursuant to confidentiality agreements, to develop, tune, enhance, and improve the Services.

Although we may attempt to notify you when changes are made to this Privacy Policy, you are responsible for periodically reviewing any changes which may be made to the Policy. We may, in our sole discretion, modify or revise the Policy at any time, and you agree to be bound by the same.

Our privacy policy is subject to change at any time without notice. To make sure you are aware of any changes, please review this policy periodically.

1. WHAT INFORMATION DOES CARE.WALLET OBTAIN?

1.1. User Provided Information and Personally Identifiable Information

- a. The Care.Wallet obtains the information you provide when you download and register the Application.
- b. When you register with us and use the Application, you generally provide your Full Name, Card Information, Phone number, Address, E-mail address. We collect general information about your use of our services. If you correspond with us by e-mail, we may retain the content of your e-mail messages, your e-mail address, and our responses. Additionally, we store information about users' contacts when users manually enter contact e-mail addresses or transfer contact information from other online social networks.

- c. Information about the Solve Token transaction;
- d. Card details to which user is subscribed to and
- e. Details of the organization to which user belongs.

1.2. Automatically Collected Information

In addition, Care.Wallet may collect certain information automatically, including, but not limited to, the type of mobile device you use, your mobile devices unique device ID, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browsers you use, and information about the way you use the Application.

2. YOUR INFORMATION AND BLOCKCHAIN

- 2.1. Blockchain technology, also known as distributed ledger technology (or simply 'DLT'), is at the core of our business. Blockchains are decentralized and made up of digitally recorded data in a chain of packages called 'blocks'. The manner in which these blocks are linked is chronological, meaning that the data is very difficult to alter once recorded.
- 2.2. Since the ledger may be distributed all over the world (across several 'nodes' which usually replicate the ledger) this means there is no single person making decisions or otherwise administering the system (such as an operator of a cloud computing system), and that there is no centralized place where it is located either. Accordingly, by design, a blockchains records cannot be changed or deleted and is said to be 'immutable'.
- 2.3. This may affect your ability to exercise your rights such as your right to erasure ('right to be forgotten'), or your rights to object or restrict processing, of your personal data. Data on the blockchain cannot be erased and cannot be changed. Although smart contracts may be used to revoke certain access rights, and some content may be made invisible to others, it is not deleted. In certain circumstances, in order to comply with our contractual obligations to you (such as delivery of tokens) it will be necessary to write certain personal data, such as your Ethereum/ bitcoin or other cryptocurrency wallet address, onto the blockchain; this is done through a smart contract and requires you to execute such transactions using your wallet's private key.
- 2.4. In most cases ultimate decisions to
 - (i) transact on the blockchain using your Ethereum/Bitcoin or other cryptocurrency wallet address, as well as
 - (ii) share the public key relating to your Ethereum/Bitcoin or other cryptocurrency wallet address with anyone (including us) rests with you.

IF YOU WANT TO ENSURE YOUR PRIVACY RIGHTS ARE NOT AFFECTED IN ANY WAY, YOU SHOULD NOT TRANSACT ON BLOCKCHAINS AS CERTAIN RIGHTS MAY NOT BE FULLY AVAILABLE OR EXERCISABLE BY YOU OR US DUE TO THE TECHNOLOGICAL INFRASTRUCTURE OF THE BLOCKCHAIN. IN PARTICULAR THE BLOCKCHAIN IS AVAILABLE TO THE PUBLIC AND ANY PERSONAL DATA SHARED ON THE BLOCKCHAIN WILL BECOME PUBLICLY AVAILABLE

3. DOES CARE.WALLET COLLECT PRECISE REAL TIME LOCATION INFORMATION OF THE DEVICE?

- 3.1. When you visit the mobile application, we may use GPS technology (or other similar technology) to determine your current location. We will not share your current location with other users or partners.
- 3.2. If you do not want us to use your location for the purposes set forth above, you should turn off the location services for the mobile application located in your account settings or in your mobile phone settings and/or within the mobile application.

4. DO THIRD PARTIES SEE AND/OR HAVE ACCESS TO INFORMATION OBTAINED BY THE APPLICATION?

- 4.1. We will share your information with third parties only in the ways that are described in this privacy statement. We may disclose User Provided and Automatically Collected Information:
 - a. As required by law
 - b. When we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a government request;
 - c. With our trusted services providers who work on our behalf, do not have an independent use of the information we disclose to them, and have agreed to adhere to the rules set forth in this privacy statement.
 - d. If Care.Wallet or the Company is involved in a merger, acquisition, or sale of all or a portion of its assets, you will be notified via email and/or a prominent notice on our Web site of any change in ownership or uses of this information, as well as any choices you may have regarding this information.

4. WHAT ARE MY OPT-OUT RIGHTS?

You can stop all collection of information by the Application easily by uninstalling the Application. You may use the standard uninstall processes as may be available as part of your mobile device or via the mobile application marketplace or network. You can also request to opt-out via email, at supportservices@solve.care.

5. DATA RETENTION POLICY, MANAGING YOUR INFORMATION

Care.Wallet will retain User provided data for as long as you use the Application and for a reasonable time thereafter. If you would like us to delete User Provided Data that you have provided via the Application, please contact us at supportservices@solve.care and we will respond within reasonable time. Please note that some or all of the User Provided Data may be required in order for the Application to function properly.

6. CHILDREN

We do not use the Application to knowingly solicit data from or market to children under the age of 13. If a parent or guardian becomes aware that his or her child has provided us with information without

their consent, he or she should contact us at supportservices@solve.care. We will delete such information from our files within a reasonable time.

7. SECURITY

We are concerned about safeguarding the confidentiality of your information. We provide physical, electronic, and procedural safeguards to protect information we process and maintain. For example, we limit access to this information to authorized employees and contractors who need to know that information in order to operate, develop or improve our Application. Please be aware that, although we endeavor to provide reasonable security for information we process and maintain, no security system can prevent all potential security breaches.

8. SPECIAL CATEGORIES OF PERSONAL DATA

- 8.1. Some of the data that you provide us may fall within what EU data protection law describes as 'special categories of personal data'.
- 8.2. We use this information in the same way we use all the other information we collect, but the law requires that we have your explicit consent to collect and use it.
- 8.3. By accepting our updated Privacy Policy, you consent to Solve.Care Foundation OÜ using this information.

9. LEGAL GROUNDS FOR PROCESSING YOUR PERSONAL DATA

- 9.1. Care.Wallet is committed to the lawful, fair and transparent use of personal data. For every use of your personal data we have described so far, we process your personal data for legitimate interests we pursue as a business.
- 9.2. If you have any questions about the grounds under which we process your personal data, or would like to find out more about the approach we take to determine that these grounds apply, please contact our Data Protection Officer using the contact details in the 'Contact Us' section.

10. TRANSFERRING PERSONAL DATA OUTSIDE THE EEA

- 10.1. We take all steps possible to ensure that your personal data remains within the European Economic Area ("EEA"). However, in some cases we need to share data with other Solve.Care Foundation OÜ group companies or third parties that are in countries outside the EEA, as described earlier. These countries may not have similar data protection laws and so they may not protect the use of your personal information to the same extent.
- 10.2. In these cases, we put in place appropriate safeguards to make sure your personal data remains adequately protected. Specifically, we make use of one of the following:
 - a. **Standard contractual clauses:** We use standard contractual clauses for the transfer of personal data to organizations outside the EEA. These contractual commitments have been adopted by the European Commission and ensure adequate protection for personal data transferred to countries outside the EEA by binding recipients of personal data to certain data protection standards including obliging them to apply appropriate technical and security measures. We use standard contractual clauses when we transfer data to other Solve.Care

Foundation OÜ Group companies and for transfers to recipients that are neither Privacy Shield certified nor located in a country covered by an adequacy decision.

- b. **EU-US Privacy Shield:** The Privacy Shield is a program agreed between the EU and US which aims to protect the personal data of anyone in the EU when it is transferred to the US by placing data protection obligations on US companies that receive personal data from the EU. Care.Wallet may rely on these safeguards when transferring data to companies based in the US where those companies are Privacy Shield certified.
- c. **Adequacy decisions:** Where the European Commission has determined that a country outside the EU offers an adequate level of data protection, personal data may be sent to that third country without implementing any other safeguards mentioned above. Care.Wallet may rely on adequacy decisions when transferring data to companies based in countries where such assurances have been given.

Please contact us using the details at the end of this notice for more information about the protections that we put in place and to obtain a copy of the relevant document.

11. RIGHTS OF THE DATA SUBJECT

a) Right of confirmation

Each data subject shall have the right granted by the European legislator to obtain from the controller the confirmation as to whether or not personal data concerning him or her are being processed. If a data subject wishes to avail himself of this right of confirmation, he or she may, at any time, contact any employee of the controller.

b) Right of access

Each data subject shall have the right granted by the European legislator to obtain from the controller free information about his or her personal data stored at any time and a copy of this information. Furthermore, the European directives and regulations grant the data subject access to the following information:

- i. the purposes of the processing;
- ii. the categories of personal data concerned;
- iii. the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- iv. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- v. the existence of the right to request from the controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing;
- vi. the existence of the right to lodge a complaint with a supervisory authority;
- vii. where the personal data are not collected from the data subject, any available information as to their source;

- viii. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.
- ix. Furthermore, the data subject shall have a right to obtain information as to whether personal data are transferred to a third country or to an international organization. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer. If a data subject wishes to avail himself of this right of access, he or she may, at any time, contact any employee of the controller.

c) Right to rectification

Each data subject shall have the right granted by the European legislator to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Considering the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. If a data subject wishes to exercise this right to rectification, he or she may, at any time, contact any employee of the controller.

d) Right to erasure (Right to be forgotten)

Each data subject shall have the right granted by the European legislator to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies, as long as the processing is not necessary:

- i. The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- ii. The data subject withdraws consent to which the processing is based according to the point (a) of Article 6(1) of the GDPR, or point (a) of Article 9(2) of the GDPR, and where there is no other legal ground for the processing.
- iii. The data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR.
- iv. The personal data have been unlawfully processed.
- v. The personal data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.
- vi. The personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.
- vii. If one of the aforementioned reasons applies, and a data subject wishes to request the erasure of personal data stored by us, he or she may, at any time, contact any employee of the controller. Any of our Employees shall promptly ensure that the erasure request is complied with immediately.
- viii. Where the controller has made personal data public and is obliged pursuant to Article 17(1) to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other

controllers processing the personal data that the data subject has requested erasure by such controllers of any links to, or copy or replication of, those personal data, as far as processing is not required. Any of our employees will arrange the necessary measures in individual cases.

However, when interacting with the blockchain, as it is a public decentralized network, we will likely not be able to prevent external parties from processing any personal data which has been written onto the blockchain. In these circumstances we will use our reasonable endeavours to ensure that all processing of personal data held by us is restricted, notwithstanding this, your right to restrict to processing may not be able to be fully enforced.

e) Right of restriction of processing

- i. Each data subject shall have the right granted by the European legislator to obtain from the controller restriction of processing where one of the following applies:
 - A. The accuracy of the personal data is contested by the data subject, for a period enabling the 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 instead of the restriction of their use instead. The 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 pursuant to Article 21(1) of the GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject. If one of the aforementioned conditions is met, and a data subject wishes to request the restriction of the processing of personal data stored by us, he or she may at any time contact any employee of the controller. Our Employees will arrange the restriction of the processing.

f) Right to data portability

- i. Each data subject shall have the right granted by the European legislator, to receive the personal data concerning him or her, which was provided to a controller, in a structured, commonly used and machine-readable format. He or she shall have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, as long as the processing is based on consent pursuant to point (a) of Article 6(1) of the GDPR or point (a) of Article 9(2) of the GDPR, or on a contract pursuant to point (b) of Article 6(1) of the GDPR, and the processing is carried out by automated means, as long as the processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- ii. Furthermore, in exercising his or her right to data portability pursuant to Article 20(1) of the GDPR, the data subject shall have the right to have personal data transmitted directly from one controller to another, where technically feasible and when doing so does not adversely affect the rights and freedoms of others.

- iii. In order to assert the right to data portability, the data subject may at any time contact any of our employee..

g) Right to object

- i. Each data subject shall have the right granted by the European legislator to object, on grounds relating to his or her particular situation, at any time, to processing of personal data concerning him or her, which is based on point (e) or (f) of Article 6(1) of the GDPR. This also applies to profiling based on these provisions. We shall no longer process the personal data in the event of the objection, unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject, or for the establishment, exercise or defence of legal claims. If we process personal data for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing. This applies to profiling to the extent that it is related to such direct marketing. If the data subject objects us to the processing for direct marketing purposes, we will no longer process the personal data for these purposes. In addition, the data subject has the right, on grounds relating to his or her particular situation, to object to processing of personal data concerning him or her by us for scientific or historical research purposes, or for statistical purposes pursuant to Article 89(1) of the GDPR, unless the processing is necessary for the performance of a task carried out for reasons of public interest.
- ii. In order to exercise the right to object, the data subject may contact any employee of our Company. In addition, the data subject is free in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, to use his or her right to object by automated means using technical specifications.

h) Automated individual decision-making, including profiling

- i. Each data subject shall have the right granted by the European legislator 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, as long as the decision (1) is not necessary for entering into, or the performance of, a contract between the data subject and a data controller, or (2) is not authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or (3) is not based on the data subject's explicit consent. If the decision (1) is necessary for entering into, or the performance of, a contract between the data subject and a data controller, or (2) it is based on the data subject's explicit consent, we shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and contest the decision.
- ii. If the data subject wishes to exercise the rights concerning automated individual decision-making, he or she may, at any time, contact any our employee.

i) Right to withdraw data protection consent

- i. Each data subject shall have the right granted by the European legislator to withdraw his or her consent to the processing of his or her personal data at any time.
- ii. If the data subject wishes to exercise the right to withdraw the consent, he or she may, at any time, contact any of our employees.

j) Right to request access

You also have a right to access information we hold about you. We are happy to provide you with details of your Personal Information that we hold or process. To protect your personal information, we follow set storage and disclosure procedures, which mean that we will require proof of identity from you prior to disclosing such information. You can exercise this right at any time by contacting us on the above details.

k) Right to withdraw consent

Where the legal basis for processing your personal information is your consent, you have the right to withdraw that consent at any time by contacting us on the above details

12. CHANGES

This Privacy Policy may be updated from time to time for any reason. We will notify you of any changes to our Privacy Policy by informing you via email or in app notifications. You are advised to consult this Privacy Policy regularly for any changes, as continued use is deemed approval of all changes.

13. CONTACT US

If you have any questions regarding privacy while using Care.Wallet, or have questions about our practices, please contact us via email at supportservices@solve.care.