

Terms of service

Riverr pte. ltd.

By using Riverr you agree that you are familiar with Terms & Conditions of our service and accept them.

Last modified: February 2021

1. Your Acceptance

This is an agreement between Riverr Pte Ltd ("Riverr") and you ("you" or "You"), a user of the Riverr Service ("Service").

BY USING THE SERVICE, YOU ACKNOWLEDGE AND AGREE TO THESE TERMS OF USE ("Terms"). If you choose to not agree with any of these terms, you may not use the Service. These terms may be modified or updated by Riverr from time to time and are effective upon posting an updated version to the Service. Continued use of the Service shall constitute your consent to such changes.

BY CLICKING THE "AGREE" BUTTON AND USING THE SERVICES YOU (A) ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT; AND (B) YOU ACCEPT THIS AGREEMENT AND AGREE THAT YOU ARE LEGALLY BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE SERVICE.



2. The Service

The role of Riverr in the Service is to provide a digital health status credentialing system. There are three (3) types of users for the Riverr platform, as below:

(i)

“Presenter”: The user of the Riverr App can store a digital copy of their health status document on their mobile device, which represents that that user is in compliance with a particular health status (“Health Status Certificate”). The Riverr App allows that Health Status Certificate to be presented to a third-party to verify this compliance. The Health Status Certificate that may be stored on the Riverr App include but are not limited to: medical certificates, test results, vaccination records and any other health related certification. It is the Presenter’s sole responsibility to ensure that they enter accurate personal details, upload valid Health Status Certificate(s) and use secure passwords for both their mobile device and the Riverr App itself in order to ensure the proper security, protection and management of any data and documentation stored on their mobile device while using the Riverr App.

(ii)

“Issuer / Attester”: The third-party service provider that digitally attests to the Health Status Certificates of Presenters in an authorised capacity. This may include, but is not limited to: medical professionals, healthcare providers and other professionals or entities authorised to provide attestation for the health-related information of individuals.

(iii)

“Verifier”: An individual or entity that uses the Riverr Wallet App to verify that a Presenter is of a particular health status, based on the information represented by a relevant and valid Health Status Certificate stored and attested to on the mobile device of a Presenter employing the Riverr App. It is the Verifier’s sole responsibility to ensure that they correctly follow the instructions for usage shown in the Riverr App, including in relation to a verification process for 3rd party Presenters.

DISCLAIMER: In the use of the Service, each of the Presenters, Attesters and Verifiers are not controlled by Riverr. Any interaction between Presenters, Attesters and Verifiers, including any medical or health-related information that each of the parties seeks to receive or provide, is between those parties and does not include Riverr. Riverr has no responsibility over the actions or inactions of Presenters, Attesters, Verifiers or any other third-party service providers.



Any service providers or other parties that need to be consulted or interacted with in relation to the Service are third-parties responsible for their own actions and inactions and are not acting at the direction of Riverr nor are subject to any control by Riverr. Riverr waives all responsibility for the actions or inactions of such service providers, particularly in relation to the accuracy and correctness of any tests, medical procedures or other health checks conducted by such service providers.

3. In-App Security

Since your Personal Health Data Status Certificate(s) are stored locally on your mobile device, Riverr Wallet users have sole responsibility for ensuring that they set up and maintain their mobile device settings at the appropriate and highest level of security. For example, you should not use the Riverr App on "rooted devices" and also should ensure that you have a passcode and/or biometric locks enabled.

4. Use of Blockchain Technology & Hash Data

In providing the Service, Riverr employs peer-to-peer blockchain technology built on the Ethereum public blockchain network ("Ethereum"), which is a global, open-source decentralised computing platform. Unlike centralised computing networks, which are supported and secured by a single or small number of private databases and/servers (or "nodes"), Ethereum is supported and secured by a decentralised public network of discrete nodes globally (the total number nodes at any given time can be seen here: <https://etherscan.io/nodetracker>). More information on Ethereum can be found here: <https://ethereum.org/en/> and on blockchain technology generally here: <https://en.wikipedia.org/wiki/Blockchain>.

Ethereum provides a platform for the deployment of decentralised applications ("Dapps") such as the Riverr Wallet, which are applications that use decentralised blockchain networks to function and access the relevant functional advantages of blockchain technology (more information on Dapps can be found here:

https://en.wikipedia.org/wiki/Decentralized_application).

In providing the Service, the Riverr Wallet employs the SHA 256 "hashing algorithm" (<https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/>) to generate "hash data" based on the personal data recorded onto the Riverr App by users. The hash data of individual Presenters is batched and compressed together with the hash data of up to 1,000 other Presenters into a single hash (known as the "Merkle Root") in a "Merkle Tree" – which is then written immutably to the Ethereum blockchain. As a result of this process, there is never a one-to-one relationship between hash data and the Presenter's individual personal data. A second piece of information (known as the "Merkle Proof"), is required to check the Presenter's hash of their Health Status Certificate is contained in the Merkle Tree. While the Merkle Proof and the hash data relating to individual Health Status Certificates is cached on the Riverr central server, it is not possible to generate a "list" of all attested hashes from our servers (in other



words, this hash data is public, but not enumerable). More information on Merkle Trees and Merkle Roots can be seen here:

<https://www.blockchain-council.org/blockchain/what-is-merkel-tree-merkel-root-in-blockchain/>.

This use of hash data forms the underlying mechanism by which third-party Verifiers are able to verify the validity of Health Status Certificates held by Presenters in a trusted manner without needing to actually access or view the personal health data of those Presenters. Unlike encryption, which allows a two-way process for encryption and de-encryption of data using an encryption algorithm, hashing works in one direction only – for a given piece of information put through a hashing algorithm, the resulting hash data cannot be used to reconstruct the original data or identify the individual to which that data refers (more information on hash data can be found here:

<https://dataspace.com/big-data-applications/what-does-it-mean-to-hash-data/>). The Health Status Certificates of Presenters are also not stored on the blockchain, but only on the mobile device of the owner of that unique digital document. Therefore, no actual private health data recorded or documentation uploaded by Presenters into the Riverr App is recorded on the Ethereum blockchain, only hash data that can be considered fully anonymised.

The key advantages of using the Ethereum blockchain in providing the Service includes:

- (i) theoretical immutability of hash data stored on the blockchain, which protects against unauthorised alteration or censoring of that hash data and
- (ii) greater security based on its reliance on a wide decentralised network of nodes rather than a single or concentrated number of nodes relied on by centralised systems, resulting in a single or concentrated points of failure. Notwithstanding this, the Ethereum blockchain is a third-party decentralised network and Riverr has no responsibility over the actions or inactions of the Ethereum blockchain.

The risks of using blockchain technology can be broadly classified under three general categories:

1. **Standard risks:** Blockchain technologies expose institutions and users to risks that are similar to those associated with current business processes and service frameworks. However, based on the inherent differences of blockchain technologies as compared to other existing centralised technologies, blockchain introduce nuances, which users and entities need to take into account. As with any technology, users and entities must make their own assessment of whether the specific functionality and characteristics are in accordance with existing policies and practices. A non-exhaustive list of examples of such standard risks includes: business continuity risk, information security risk, regulatory risk,



operational/IT risks, contractual risks and third-party supplier risks.

2. **Data transfer risks:** Blockchain enables peer-to-peer transfer of data without the need for a central intermediary. This model for data storage and sharing exposes the interacting parties to new risks that were previously managed by central intermediaries. A non-exhaustive list of examples of such data transfer risks includes: blockchain protocol risks, private key management risks and data confidentiality risks.
3. **Smart contract risks:** Smart contracts encode complex business, financial, and legal arrangements on the blockchain, and could result in the risk associated with the one-to-one mapping of these arrangements from the physical to the digital framework. A non-exhaustive list of examples of such smart contract risks includes: business process risks, regulatory risks, contract enforcement risks, legal liability risks and information security risks.

Riverr, in developing the Service, has made all reasonable efforts to address the risks it has identified, which are associated with the use of blockchain technology. However, blockchain technology is a complex and relatively new technology. Therefore, there may be new and additional risks and/or technical vulnerabilities not originally envisaged that arise in future. Riverr disclaims all liability based on the inherent and potentially undefined risks associated with blockchain technology and encourages all users and entities employing the Riverr App to fully assess the attendant risks for themselves before accepting these Terms of Use.

5. Use of External Data Service Providers

In providing the Service, Riverr employs AWS (<https://aws.amazon.com/>) as third-party service provider to securely store specific user data on an encrypted external database, including:

- Email addresses of authorised Attestors in hashed and encrypted format;
- Merkel Proofs and Merkel Roots in relation to hashed Health Status Certificates to enable the verification process provided by the Service; and
- A cache of hashes relating to Health Status Certificates that correlates to the hashed emails of Attestors to enable traceability of Attestation as provided by the Service.

The storage of this user data is necessary to enable traceability of all attestations made by Attestors in relation to the Health Status Certificates of Presenters, for the purposes of detecting and preventing fraudulent attestations. Details of AWS's Data Processing disclosures and protections can be found here:

<https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/>.



6. Collection and Use of Your Information

You will be required to provide certain information (“Content”) about yourself as a condition to using the Service and creating a profile on the Riverr App. All Content that you provide will be stored on your mobile device and not on any external database or server and is subject to the Riverr Privacy Policy. By using the Service, you consent to all actions taken by Riverr with respect to the Content in compliance with this Privacy Policy and the laws of the Republic of Singapore. You represent and warrant that (i) You will comply with all the laws of the Republic of Singapore pertaining to the Content (ii) that you have the right to upload the Content to the Riverr App and (iii) that your use of the Content does not infringe on any rights of any third-party.

DISCLAIMER: Any service providers or other parties that need to be consulted or interacted with in relation to the Service are third-parties responsible for their own actions and inactions and are not acting at the direction of Riverr nor are subject to any control by Riverr. Riverr waives all responsibility for the actions or inactions of such service providers, particularly in relation to the accuracy and attestation of Health Status Certificates stored on the Riverr App.

7. Service Access

A. Subject to your compliance with these Terms, Riverr hereby grants you permission to use the Service, provided that: (i) your use of the Service as permitted is solely for your personal use, and you are not permitted to resell or charge others for use of or access to the Service, or in any other manner inconsistent with these Terms; (ii) you will not duplicate, transfer, give access to, copy or distribute any part of the Service in any medium without Riverr’ prior written authorization; (iii) you will not attempt to disassemble, decompile, prepare derivative works of, reverse engineer, alter, modify or attempt to gain access to the source code of any part of the Service; and (iv) knowingly or negligently use the Service in a way that abuses interferes with or disrupts Riverr’ networks or the Service; (v) engage in activity that is illegal, fraudulent, false or misleading; (vi) build or benchmark a competitive product or service, or copy any features, functions or graphics of the Service or (vii) use the Service to communicate any message or material that is harassing, libellous, threatening, obscene, indecent, would violate the intellectual property rights of any party or is otherwise unlawful, that would give rise to civil liability, or that constitutes or encourages conduct that could constitute a criminal offense, under any applicable law or regulation; and (viii) upload or transmit any software, Content or code that does or is intended to do harm, disable, destroy or adversely affect performance of the Service in any way or which does or is intended to harm or extract information or data from other hardware, software of Riverr and/or other users of the Service.

B. Riverr will maintain reasonable physical and technical safeguards to prevent unauthorized disclosure of or access to Content, in accordance with commercially reasonable standards. This includes the encryption of any data or Content stored on Riverr servers. You must notify Riverr immediately of any breach of security or unauthorized use of your mobile device with the Riverr App installed. Although Riverr will not be liable for your losses caused by any unauthorized use



of your account, you may be liable for the losses of Riverr or others due to such unauthorized use.

C. Termination of the Service can be implemented by you by deleting all Content and Health Status Certificate(s) stored on your Riverr App or by simply uninstalling the Riverr App from your mobile device. As all personal health data and digital documentation is stored only on your mobile device, this deletion or uninstallation will result in the permanent loss of all that data and documentation. Any hash data relating to your personal health data will remain written to the Ethereum public blockchain but it will not be possible to use that hash data to identify you or recreate the personal data or digital documentation deleted by you.

8. Intellectual Property Rights

The design of the Service along with Riverr trade name, trademarks, service marks logos and domain names ("Riverr Marks"), are owned by Riverr and/or Riverr' suppliers who retain ownership of all proprietary rights therein. You may not make any use of any Riverr Marks without express written consent.

9. Export Regulation

The Service, or portion thereof may be subject to the export control laws of the United States and other applicable country export control and trade sanctions laws ("Export Control and Sanctions Laws"). You may not access, use, export, divert, transfer or disclose any portion of the Service or any related technical information or materials, directly or indirectly, in violation of any applicable export control or trade sanctions law or regulation. You represent and warrant that (i) You are not citizens of, or located within, a country or territory that is subject to U.S. trade sanctions or other significant trade restrictions (including without limitation Cuba, Iran, North Korea, Syria and the Crimea) and that You will not access or use the Service, or export, re-export, divert, or transfer the Service in or to such countries or territories; (ii) You are not identified on any U.S. government restricted party lists and (iii) that no Content created or submitted by You is subject to any restriction or disclosure, transfer, download, export or re-export under the Export Control Laws.

10. Warranty Disclaimer

YOU UNDERSTAND AND AGREE THAT THE SERVICE IS PROVIDED "AS IS", WITH ALL FAULTS AND DEFECTS AND WITHOUT WARRANTY OF ANY KIND. RIVERR, ON ITS OWN BEHALF ON BEHALF OF ITS AFFILIATES AND SUPPLIERS EXPRESSLY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND WARRANTIES THAT MAY ARISE OUT OF COURSE OF DEALING, COURSE OF PERFORMANCE, USAGE, OR TRADE PRACTICE. IN CONNECTION WITH THE SERVICE AND YOUR USE THEREOF. Riverr PROVIDES NO



WARRANTY OR UNDERTAKING, AND MAKES NO OR REPRESENTATION REGARDING THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE SERVICE.

11. Limitation of Liability

TO THE EXTENT PERMITTED BY APPLICABLE LAW YOU WAIVE ALL CLAIMS AGAINST Riverr, ITS PARTNERS, AFFILIATES AND SUPPLIERS FOR ANY LOSS TO THE EXTENT ARISING FROM ANY ADVICE GIVEN IN CONNECTION WITH THE SERVICE. IN NO EVENT SHALL Riverr, ITS OFFICERS, DIRECTORS, EMPLOYEES, OR AGENTS, BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES WHATSOEVER RESULTING FROM ANY (I) ERRORS, MISTAKES, OR INACCURACIES OF CONTENT, (II) PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM YOUR ACCESS TO AND USE OF THE SERVICE, (III) ANY UNAUTHORIZED ACCESS TO OR USE OF OUR SECURE SERVERS AND/OR ANY AND ALL PERSONAL INFORMATION AND/OR FINANCIAL INFORMATION HELD THEREIN, (IV) ANY INTERRUPTION OR CESSATION OF TRANSMISSION TO OR FROM OUR SERVERS, (V) ANY BUGS, VIRUSES, TROJAN HORSES, OR THE LIKE, WHICH MAY BE TRANSMITTED TO OR THROUGH OUR SERVICE BY ANY THIRD PARTY, (VI) ANY ERRORS OR OMISSIONS IN ANY CONTENT OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF YOUR USE OF ANY CONTENT TRANSMITTED, OR OTHERWISE MADE AVAILABLE VIA THE SERVICE, WHETHER BASED ON WARRANTY, CONTRACT, TORT, OR ANY OTHER LEGAL THEORY, AND WHETHER OR NOT THE COMPANY IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND/OR (VII) THE DISCLOSURE OF INFORMATION PURSUANT TO THESE TERMS . THE FOREGOING LIMITATION OF LIABILITY SHALL APPLY TO THE FULLEST EXTENT PERMITTED BY LAW IN THE APPLICABLE JURISDICTION.

The Service is controlled and offered by Riverr in selected locations. Those who access or use the Service do so at their own volition and are responsible for compliance with the local law of the Republic of Singapore.

12. Indemnity

You agree to defend, indemnify and hold harmless Riverr, its parent corporation, officers, directors, employees and agents, from and against any and all claims, damages, obligations, losses, liabilities, costs or debt, and expenses (including but not limited to attorney's fees) arising from: (i) your use of and access to the Service; (ii) your violation of any term of these Terms; or (iii) your violation of any third party right, including without limitation any copyright, property, or privacy right. This defence and indemnification obligation will survive these Terms and your use of the Service.



13. General

These Terms shall be governed by the substantive laws of the Republic of Singapore, without regard to conflict of laws principles. These Terms shall constitute the entire agreement between you and Riverr concerning the Service. If any provision of these Terms is deemed invalid by a court of competent jurisdiction, the invalidity of such provision shall not affect the validity of the remaining provisions of these Terms, which shall remain in full force and effect. No waiver of any term of these Terms shall be deemed a further or continuing waiver of such term or any other term, and Riverr' failure to assert any right or provision under these Terms shall not constitute a waiver of such right or provision. Riverr reserves the right to amend or modify these Terms at any time, and it is your responsibility to review these Terms for any changes. If you do not agree to the revised Terms, your only recourse is to discontinue the use of the Service. Your continued use of the Service following any amendment of these Terms will signify your assent to and acceptance of its revised terms. YOU AND Riverr AGREE THAT ANY CAUSE OF ACTION ARISING OUT OF OR RELATED TO THE SERVICE MUST COMMENCE WITHIN ONE (1) YEAR AFTER THE CAUSE OF ACTION ACCRUES. OTHERWISE, SUCH CAUSE OF ACTION IS PERMANENTLY BARRED.

