

Privacy Policy

LightLink Network Limited and its affiliates (hereinafter referred to as, “LightLink”, “we or our”) is committed to safeguarding personal data. This Privacy Policy relates to our use and collection of personal information and data relating to visitor and user who visits, access and/or use this website (“Website”) or any LightLink’s application or network (hereinafter referred to as “you”, “your” or “user”). With respect to user, LightLink is the data controller of your personal information processed under this Privacy Policy. This Privacy Policy provides you with detail about how we use your personal information. We use commercially reasonable physical, electronic and procedural measures to protect your personal information in accordance with data protection legislative requirements, i.e., General Data Protection Regulation 2016/679, and/or any data protection regulation in a competent jurisdiction. This Privacy Policy does not apply to anonymized data as it cannot be used to identify you. We will not use your personal information for purposes other than those purposes we have disclosed to you in this Privacy Policy without your permission. By visiting, accessing or using our applications, blockchain network, our Website and/or any features on the Website, you acknowledge that we use your personal information as set out in this Privacy Policy. Unless stated otherwise, we adopt in this Privacy Policy the defined terms used in the Term of Use (<https://lightlink.io/terms-of-use>).

1. We Value Your Privacy

This Privacy Policy is intended to explain our privacy practices and covers the following areas:

- What personal information about you we may collect;
- Our use of cookies and similar technology;
- How we may use your personal information;
- Whom we may disclose your personal information to;
- Our use of automated decision-making;
- How we protect your personal information;
- How to contact us;
- Your rights to prevent marketing and to access and update your personal information; and
- How changes to this Privacy Policy and the Cookies Policy will be made.

By agreeing to this Policy through your continued use of our services and access to the Website, you agree to the terms and conditions of this Privacy Policy.

2. Information We May Collect About You (Collectively, “Personal Data”)

2.1. We may collect the following personal information from you when you access with our applications, access with our network or register with us:

- Contact Information: name, email address, username or profile link to Facebook, Google, X (formerly known as Twitter) and/or certain social network services
- Account information: username and password
- Financial Information: your Ethereum network address, cryptocurrency wallet information, transaction history, trading data, etc.
- Correspondence: your feedback, response, and any information you provided to our team via various channels, including social media channels.

2.2. We may also automatically collect certain computer, device and browsing information when you access our website and/or our application or network:

- Online identifiers: computer or mobile device information, including internet protocol (IP) address, operating system, browser type and version, internet service provider (ISP)
- Website usage information: user preferences, interaction with others on the Website including any comments or posts that you make in our public discussion forums, photos or media that you upload to the Website, any other contents that you may provide to the Website and other data collected via cookies and similar technologies, referring/exit pages, operating system, date/time stamp, clickstream data, etc.
- Location information or tracking details
- Transaction information: the transaction information you made on LightLink applications and network, transaction amount and timestamp

2.3. We may also collect personal information about you from public databases or third party partner including: Reputational information or financial information status on any politically exposed person and sanctions lists digital asset transaction record business activities of corporate users other information to help validate your identity.

2.4. We also collect personal information disclosed by you when you contact us or respond to our communications (e.g., email, social media, the contents of a message or attachments that you may send to us and/or other information that you choose to provide when you contact us).

3. Uses Made of Your Personal Information

3.1. We may use your personal information in the ways listed below:

- To provide, personalize, maintain and improve our Website, service, applications effectively to users; to administer, operate, maintain, customize, measure and improve our Website, applications and network; to create and update users' accounts; to process transaction; to send information including confirmations, notices, updates, security alerts and support and administrative messages; and to create de-identified or aggregated data.
- To develop our products and services; to evaluate new products and services and to improve our service quality, including by performing statistical analysis and reporting on transactions and Website usage.
- For financial reporting, management reporting, audit and record keeping purposes.
- To manage our risk: We may use your personal information in managing the risk of our user, including for assessing and processing applications, instructions or requests from you, maintaining our infrastructure and complying with internal policies and procedures and monitoring the use of our Website.
- To verify your identity: If you are registering an account with us, for the purposes of providing products or services, including conducting screenings or due diligence checks as may be required under applicable law, regulation, directive or our Terms of Use.
- To provide safety and security for user and prevent fraud: We and other organizations may also access and use certain information to maintain the safety, security and integrity of you and our Website, and to prevent fraud as may be required by applicable law and regulation and best practice at any given time. Such use of information may include (i) to protect, investigate and deter against fraudulent, unauthorized or illegal activity; (ii) to monitor and verify identity or Website access, combat spam, malware or security risks; (iii) to perform internal operations necessary to provide our Website, including to troubleshoot software

bugs and operational problems; (iv) to enforce our agreement with third parties and address violations of our Terms of Use; and (v) to comply with applicable security laws and regulations. If false or inaccurate information is provided or fraud is identified or suspected, details may be passed to law enforcement and fraud prevention agencies and may be recorded by us or by them.

- In connection with legal or regulatory obligations: We may share your information with law enforcement, regulatory authorities and officials, or other third parties when we are compelled to do so by a subpoena, court order, or similar legal procedure, or when we believe in good faith that the disclosure of personal information is necessary to prevent physical harm or financial loss, to report suspected illegal activity or to investigate violations of our Terms of Use or any other applicable policies. We may also use your personal information to otherwise comply with all applicable laws, regulations, rules, directives and orders.
- In order to communicate with you: We may use your personal information to communicate with you, including providing you with updates on changes to Website, products and services including any additions, expansions, suspensions and replacements of or to such features on the Website.
- In connection with disputes: We may use your personal information to address or investigate any complaints, claims or disputes and to enforce obligations owed to us.
- For research and development: We may use the information we collect for testing, research, analysis and product development to improve your experience. This helps us to improve and enhance the safety and security of our Website, improve our ability to prevent the use of our Website for illegal or improper purposes and develop new features and products.
- For marketing: Subject to applicable laws and regulations, we may use your personal information (including your on-chain addresses and/or social media information (such as, but not limited to, your email address, X (formerly known as Twitter) account, etc.) to inform our marketing strategy and to tailor our messaging to your needs. Where required by law, we will ask for your consent at the time we collect your data to conduct such marketing. An opt-out mechanism will be provided to you in each communication to enable you to exercise your right to opt out of any direct marketing. We never sell your information. You may withdraw this consent/opt-out at any time without affecting the lawfulness of processing based on your prior consent.

3.2. We do not rent, sell or share your information with third parties except as described in this Privacy Policy. We may share your information with the following:

- Entities in our group or our affiliates in order to provide you with our services;
- Our third party service providers who provide services such as website hosting, data storage, data analysis, customer services, email delivery, auditing, and other services;
- Credit bureaus and other third parties who provide Know-Your-Customer (KYC) and Anti-Money Laundering (AML) services;

- Potential or actual acquirer, successor, or assignee as part of any reorganisation, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in bankruptcy or similar proceedings); and/or
- If required to do so by law or in the good faith belief that such action is appropriate: (i) under applicable law, including laws outside your country of residence; (ii) to comply with legal process; (iii) to respond to requests from public and government authorities, including public and government authorities outside your country of residence; (iv) to enforce our terms and conditions; (v) to protect our operations or those of any of our subsidiaries; (vi) to protect our rights, privacy, safety or property, and/or that of our subsidiaries, you or others; and (vii) to allow us to pursue available remedies or limit the damages that we may sustain.

4. Automated Decision-Making

Our operation of the Website relies on automated analysis of personal information provided by you, alongside that received from AML and fraud prevention agencies. For more information on the anti-fraud measures adopted by us, please see section 7 of this Privacy Policy. We may use criteria such as your identifying information (e.g., your name, email address, wallet address, or other information) to validate your identity against public records on an automated basis or without human/manual intervention. We do this on the basis that it is necessary for us to enter into a contract with you. If you fail to meet these criteria, your application to use our Website will be rejected. You may also request that we provide information about our methodology and ask us to verify that the automated decision has been made correctly. We may reject the request, as permitted by applicable law, including when providing the information would result in a disclosure of a trade secret or would interfere with the prevention or detection of fraud or other crime. However, generally in these circumstances we will verify (or request the relevant third party to verify) that the algorithm and source data are functioning as anticipated without error or bias.

5. Transmission, Storage and Security of your Personal Information over the Internet

5.1. No data transmission over the Internet or website can be guaranteed to be secure from intrusion. However, we maintain commercially reasonable physical, electronic and procedural safeguards to protect your personal information in accordance with data protection legislative requirements.

5.2. All information you provide to us is stored on our or our service providers' secure servers and accessed and used subject to our security policies and standards. Where we have given you (or where you have chosen) a password that enables you to access certain parts of our websites, you are responsible for keeping this password confidential and for complying with any other security procedures that we notify you of. We ask you not to share a password with anyone.

5.3. Your personal information may be accessed by staff or suppliers in, transferred to, and/or stored at, a destination outside of European Union in which data protection laws may be of a lower standard. Regardless of location or whether the person is an employee or contractor, we will impose the same data protection safeguards that we deploy herein.

5.4. We will retain your personal information for as long as is necessary for the processing purpose(s) for which they were collected and any other permitted linked purpose (for example certain transaction details and correspondence may be retained until the time limit for claims in respect of the transaction has expired or in order to comply with regulatory requirements regarding the retention of such data). So if information is used for two purposes, we will retain it until the purpose

with the latest period expires; but we will stop using it for the purpose with a shorter period once that period expires.

5.5. We restrict access to your personal information to those persons who need to use it for the relevant purpose(s). Our retention periods are based on business needs, and your information that is no longer needed is either irreversibly anonymised (and the anonymised information may be retained) or securely destroyed.

By way of example:

- use to perform a contract: in relation to your personal information used to perform any contractual obligation to you, we may retain that personal information whilst the contract remains in force plus a further period (depending on jurisdiction and other factors) to deal with any queries or claims thereafter;
- copies of evidence obtained in relation to AML checks: in relation to your personal information obtained in relation to AML checks, we may retain that personal information in force for a 7 years to deal with any queries or claims thereafter; and
- where claims are contemplated: in relation to any information where we reasonably believe it will be necessary to defend or prosecute or make a claim against you, us or a third party, we may retain that information for as long as that claim could be pursued.

5.6. Digital Assets may not be fully anonymous as a result of the public digital ledgers reflecting these assets. Generally, anyone can view the balance and transaction history of any public wallet address. We, and others who are able to match your public wallet address to other information about you, and also may be able to identify you from a blockchain transaction. Furthermore, third parties may use data analytics to identify other information about you. Please note that such third parties have their own privacy policies and that we do not accept any responsibility or liability for their policies or processing of your personal information.

5.7. You need to help us prevent unauthorised access to your account by protecting and limiting access to your account appropriately (for example, by logging out after you have finished accessing your account). You will be solely responsible for keeping your account against any unauthorised use. While we seek to protect your information to ensure that it is kept confidential, we cannot absolutely guarantee its security. Please be aware that no security measures are perfect or impenetrable and thus we cannot and do not guarantee the security of your data. While we strive to protect your personal information, we cannot ensure or warrant the security and privacy of your personal information or other content you transmit using our Website, and you do so at your own risk. It is important that you maintain the security and control of your account credentials.

6. Your Statutory Rights

6.1 Access: you are entitled to ask us if we are processing your information and, if we are, you can request access to your Personal Data. This enables you to receive a copy of the Personal Data we hold on you and certain other information about it to check that we are processing it lawfully. We process a large quantity of information and can thus request, in accordance with the regulations, that before the information is delivered, you specify the information or processing activities to which your request relates.

6.2 Correction: you are entitled to request that any incomplete or inaccurate Personal Data we hold about you is corrected.

6.3 Erasure: you are entitled to ask us to delete or remove Personal Data in certain circumstances. There are also certain exceptions where we may refuse a request for erasure; for example, where the Personal Data is required for compliance with law or in connection with claims.

6.4 Restriction: you are entitled to ask us to suspend the processing of certain parts of your Personal Data; for example, if you want us to establish its accuracy or disclose the reason for processing it.

6.5 Transfer: you may request the transfer of a certain part of your Personal Data to another party.

6.6 Objection: where we are processing your Personal Data based on a legitimate interest (or that of a third-party) you may challenge this. However, we may be entitled to continue processing your information based on our legitimate interests or where this is relevant to legal claims. You also have the right to object where we are processing your Personal Data for direct marketing purposes. We will inform you if we intend to use your information for such purposes or if we intend to disclose your information to any third party for such purposes. You can exercise your right to prevent such processing by not checking certain boxes on our marketing consent form. You can also exercise the right at any time by contacting us as set out below.

7. Processing for AML & Fraud Prevention and Detection Purposes

7.1 Before we provide our services under the Website to you, we undertake checks for the purposes of preventing fraud and money laundering. These checks require us to process personal information about you.

7.2. The personal information you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and money laundering and may be used to verify your identity.

7.3 In order to do so, we may provide information to, obtain information from, and verify information with fraud prevention and any enforcement agency. We will continue to exchange information with such parties while you have a relationship with us.

7.4. We enable law enforcement agencies to access and use your personal information to detect, investigate and prevent crime.

7.5. AML and enforcement agency can hold your personal information for different periods of time, and if you are considered to pose a fraud or money laundering risk, your data can be held for up to seven years.

7.6. As part of the processing of your personal information, decisions may be made by automated means. This means we may automatically decide that you pose a fraud or money laundering risk if our processing reveals your behavior to be consistent with money laundering or known fraudulent conduct, or is inconsistent with your previous submissions, or you appear to have deliberately hidden your true identity. You have rights in relation to automated decision making as set out in section 4 of this policy.

7.7. As a consequence of processing, if we, or a AML & enforcement agency, determine that you pose a fraud or money laundering risk, we may refuse to allow you to access part of the Website or we may stop providing existing services to you.

8. Cookies Policy

8.1. When you access our Website, we may collect information from you through automated means, such as cookies, web beacons and web server logs. By using and accessing the Website, you consent to the placement of cookies, beacons and similar technologies in your browser and on emails in accordance with this Privacy Policy. The information collected in this manner includes IP address, browser characteristics, device IDs and characteristics, operating system version, language preferences, referring URLs, and information about the usage of our services.

8.2. Cookies are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the website. Cookies are typically stored on your computer's hard drive. You may also wish to refer to <http://www.allaboutcookies.org/manage-cookies/index.html>.

8.3. We may use this information, for example, to administer the Website, to ensure that our Website functions properly, to evaluate the effectiveness of our Website, to determine how many users have visited certain pages or opened messages and what difficulties our visitors may experience in accessing our Website, or to prevent fraud. We also work with analytics providers which use cookies and similar technologies to collect and analyse information about use of the Website and report on activities and trends. With this knowledge, we can improve the quality of your experience on the Website by recognising and delivering more of the most desired features and information, as well as by resolving access difficulties. We also use cookies and/or a technology known as web bugs or clear gifs, which are typically stored in emails to help us confirm your receipt of, and response to, our emails and to provide you with a more personalized experience when using our Website.

8.4. We may use one or more third-party service providers, to assist us in better understanding the use of our Website. Our service provider(s) will place cookies on the hard drive of your computer and will receive information that we select that will educate us on such things as how visitors navigate around our Website, what page are browsed and general transaction information. Our service provider(s) will analyse this information and provide us with aggregate reports. The information and analysis provided by our service provider(s) will be used to assist us in better understanding our visitors' interests in our Website and how to better serve those interests. The information collected by our service provider(s) may be linked to and combined with information that we collect about you while you are using the Website. Our service provider(s) is/are contractually restricted from using the information they receive from our Website for any other purpose than to assist us. Our service provider(s) may set and access their own cookies, pixel tags and similar technologies on our Website and they may otherwise collect or have access to information about you which they may collect over time and across different websites.

8.5. If you do not want information collected through the use of cookies, there is a procedure in most browsers that allows you to automatically decline cookies or be given the choice of declining or accepting the transfer to your computer of a particular cookie (or cookies) from a particular site. If, however, you do not accept cookies, you may experience some inconvenience in your use of the services from our Website.

9. Changes to our Privacy Policy and/or Cookies Policy

We may change the content of our Privacy Policy from time to time in the future. We therefore encourage you to review this policy from time to time to stay informed of how we are using personal information. This Privacy Policy was last updated on 18 March 2024.

If you have any questions about this Privacy Policy, please contact us at legal@lightlink.io.