Privacy Policy

1. **GENERAL**

1.1. This Privacy Policy, together with the TARA, the Portal Terms and the KYC Requirements, governs Asynq's collection, processing and use of your Personal Data.

1.2. As used in this Privacy Policy, "**Asynq**", "**we**", "us**"** or "**our**" refers to Asynq Limited, a limited liability company registered within the England and Wales Companies Registrar under the number 12758278, with its registered address at 2nd Floor Regis House, 45 King William Street, London, United Kingdom, EC4R 9AN. Asynq is a data controller under this Privacy Policy, which sets out the manner in which it, as data controller, may use your Personal Data.

1.3. This Privacy Policy covers our use of your Personal Data arising from your use of the Portal, your creation of an Account and/or the Services we provide to you from time to time.

2. PURPOSE OF PRIVACY POLICY

2.1. Asynq is committed to protecting and respecting your privacy. The purpose of this Privacy Policy is to describe:

2.1.1. the types of Personal Data we collect and how it may be used;

2.1.2. our use of cookies and similar technology;

2.1.3. how and why we may disclose your Personal Data to third parties;

2.1.4. the transfer of your Personal Data within and outside of the EEA;

2.1.5. your statutory rights concerning your Personal Data;

2.1.6. the security measures we use to protect and prevent the loss, misuse or alteration of Personal Data; and

2.1.7. Asynq's retention of your Personal Data.

2.2. Please contact us at info@asynq.one should you require more information on our Privacy Policy.

3. **DEFINITIONS**

3.1. In this Privacy Policy, unless the context otherwise requires, the following definitions apply:

Account	a customer identification account hosted on the Portal to hold UX Tokens and access and use the UX Network
DP Law	any legal instrument applying to Asynq that applies to the processing of Personal Data including but not limited the EU General Data Protection Regulation 2016/679, its successors or implementing texts and any other laws, regulations, notices, circulars, policy statements or regulatory guidance as issued, amended or updated from time to time
EEA	European Economic Area

KYC Requirements	the rules and requirements for 'know your client' and 'anti-money laundering' verification and ongoing compliance for all Account holders as administered and enforced by Asynq (as updated or amended from time to time)
KYC Verified/Verification	the verification of your 'Know Your Client' particulars in accordance with the KYC Requirements
Personal Data	any information from which a person can be identified or potentially identified. Personal Data does not include anonymised and/or aggregated data that does not identify a specific user
Portal	the online portal hosted at www.uxnetwork.io or such other address from time to time where Accounts are created and accessed
Portal Terms	the terms and conditions that apply to parties accessing the Portal as updated or amended from time to time
Privacy Policy	this document as updated or amended by us from time to time in accordance with its terms
Services	the KYC Verification by us at Account creation and as maintained by us from time to time thereafter
TARA	the token allocation request agreement whereby a natural or legal person requests an allocation of UX Tokens
UX Network	the public blockchain known as the UX Network that allows for peer to peer transactions and the development of distributed applications
UX Token/s	the cryptographic utility tokens that represent units of network capacity of the UX Network

4. COLLECTION AND USE OF PERSONAL INFORMATION

Personal Data We Collect

4.1. We collect the Personal Data which you provide directly to us or which is generated when you open an Account, perform any actions on the Portal, or otherwise use or receive the Services from time to time. This may include:

4.1.1. contact information, such as name, home address and email address;

4.1.2. Account information, such as username, password, Account settings and preferences;

4.1.3. financial information, such as bank account numbers, bank statement and trading information;

4.1.4. identity verification information, such as images of your government-issued ID, passport, national ID card or driving licence. Note: US residents may be asked to provide their social security numbers;

4.1.5. residence verification information, such as utility bill details or similar information;

4.1.6. information that we receive from third parties including third parties who provide services to you or us, fraud prevention or government agencies;

4.1.7. information that we learn about you through our relationship with you and the way you operate your Accounts and/or services, such as the payments made to and from your Accounts;

4.1.8. information that we gather from the technology which you use to access our services (for example location data from your mobile phone, or an IP address or telephone number) and how you use it (for example pattern recognition);

4.1.9. information that we gather from publicly available sources, such as the press, the electoral register, company registers and online search engines.

4.1.10. information regarding the way in which you use our Services, such as when you used our Services, and the specific Services used; and

4.1.11. information relating to communications with us, whether through the Portal or via e-mail, over the phone or via any other medium.

4.2. We also automatically collect certain computer, device and browsing information when you access the Portal or are provided with the Services. This information is aggregated to provide statistical data about our users' browsing actions and patterns, and does not personally identify individuals. This information may include:

4.2.1. computer or mobile device information, including IP address, operating system, network system, browser type and settings; and

4.2.2. website usage information.

4.3. Finally, we may collect Personal Data from third-party partners and public sources, which include:

4.3.1. reputational information;

4.3.2. financial information;

4.3.3. business activities of corporate customers.

4.4. We need to collect certain types of information for compliance with legal requirements relating to our anti-fraud/anti-money-laundering/counter-financing-of-terrorism/know-your-customer obligations. If this information is not provided we may not be able to provide the Services to you. Your Personal Data may also be processed if it is necessary on reasonable request by a law enforcement or regulatory authority, body or agency or in the defence of legal claims. We will not delete Personal Data if relevant to an investigation or a dispute. It will continue to be stored until those issues are fully resolved.

4.5. It is important to note that the Personal Data we collect on you when you create an Account will be retained for the mandatory retention period set forth by applicable law, including DP Law, as it is necessary for us to maintain an exhaustive documentation of our operations as required, even if your Account has not been successfully activated (e.g. if Account verification/KYC Verification has not been completed) or no transaction has been made using it.

Use of Cookies and Similar Technology

4.6. The Portal uses cookies. 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 site.

4.7. The information collected from cookies allows us to determine such things as which parts of the Portal are most visited and what difficulties our visitors may experience in accessing the Portal. With this knowledge, we can improve the quality of your experience on the Portal 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 the Portal.

4.8. If you want to avoid using cookies altogether, you can disable cookies in your browser. However, disabling cookies might make it impossible for you to use certain features of the Portal or Services, such as logging in to your Account. Your use of the Portal or Service with a browser that is configured to accept cookies constitutes an acceptance of our and third-party cookies.

How We Use Your Personal Data

4.9. We collect and use your Personal Data for a variety of reasons. We need your Personal Data primarily to create your Account and provide the Services. Some information processing is required by law due to our anti-fraud screening obligations, or is in the public interest, such as making sure we verify our customers' identities.

4.10. Some Personal Data is processed because you have given your consent, which can be withdrawn in your Account preferences and settings. Other Personal Data we collect and use because we have legitimate business interests to do so, having taken into account your rights, interests and freedoms.

4.11. We may use your Personal Data to:

4.11.1. create and administer your Account and generally for Account maintenance, legal documentation records and claim and dispute management. Related processing operations are necessary for the performance of a contract with you (or to take steps at your request prior to entering into a contract) and for compliance with legal obligations to which we are subject;

4.11.2. Process your Asynq transactions. Related processing operations are necessary for the performance of a contract with you and for compliance with legal obligations to which we are subject;

4.11.3. Verify your identity in accordance with applicable know-your-customer, money-laundering and other financial sector legislation or regulations, including those required for compliance with Asynq's Anti-Money Laundering Policy, as well as address other law enforcement needs as described in our Portal Terms, and generally as required for compliance with legislation and regulations applicable to Asynq. With respect to US residents, we also may share your information with certain financial institutions, as authorized under Section 314(b) of the US Patriot Act, and with tax authorities, including the US Internal Revenue Service, pursuant to the Foreign Account Tax Compliance Act ("FATCA"), to the extent that this statute may be determined to apply to Asynq. Related processing operations are necessary for the performance of a contract with you and for compliance with legal obligations to which we are subject;

4.11.4. Personalise your Services experience. Related processing operations are necessary for purposes of our legitimate interests (that is, improving our Services);

4.11.5. Analyse Portal usage and improve the Portal and website offerings. Related processing operations are necessary for purposes of our legitimate interests (that is, improving and promoting our Services);

4.11.6. Help us respond to your customer service requests and support needs. Related processing operations are necessary for the performance of a contract with you and for purposes of our legitimate interests (that is, improving our Services and offering you the best experience);

4.11.7. Contact you about Services. The email address you provide may be used to communicate information and updates related to your use of Services.

Automated Decision Making

4.12. We may make automated decisions on certain matters. For example, we may do this to decide whether we can provide our Services to you based on a credit check/risk profiling. Depending on the outcome of the credit check/risk profiling, a decision is reached automatically as to whether we are able to provide the Services to you based on your credit worthiness.

4.13. If you disagree with the decision you are entitled to contest this by contacting us at the following email address: info@asynq.one

Marketing

4.14. We may also communicate company news, updates, promotions and information relating to similar products and Services provided by Asynq. We may also administer a contest, promotion, survey or another site feature. We shall only do this where you have given us your consent or otherwise where we are permitted to do so under DP Law in pursuit of our legitimate interests (that is, promoting our Services).

4.15. We may share Personal Data with third parties to help us with our marketing and promotional projects, or sending marketing communications.

4.16. If you want to opt out of receiving promotional and marketing emails, text messages, posts and other forms of communication from us (or our promotional partners), which you might receive in accordance with this section, you can choose one of the following ways:

4.16.1. Log into your Account and update your profile;

4.16.2. Click “unsubscribe” at the bottom of an email we sent you; or

4.16.3. Contact us at info@asynq.one and request to opt out.

4.17. If you do opt out of receiving promotional and marketing messages, we can still contact you regarding our business relationship with you, such as Account status and activity updates, survey requests in respect of products and Services we have provided to you after you have opted out or respond to your inquiries or complaints, and similar communications.

5. DISCLOSING AND TRANSFERRING PERSONAL DATA

5.1. We may disclose your Personal Data to third parties and legal and regulatory authorities and transfer your Personal Data outside the EEA, as described below.

Disclosures to Third Parties

5.2. There are certain circumstances where we may transfer your Personal Data to employees, contractors and to other parties.

5.3. We may share information about you with other members of our group of companies so we can provide the best service across our group. They are bound to keep your information in accordance with this Privacy Policy;

5.4. We may also share your information with certain contractors or service providers. They may process your Personal Data for us, for example, if we use a marketing agency. Other recipients/service providers include advertising agencies, IT specialists, credit reference agencies, screening agencies database providers, backup and disaster recovery specialists, email providers or outsourced call centres. Our suppliers and service providers are required to meet our standards on processing information and security. The information we provide them, including your information, will only be provided in relation to the performance of their function;

5.5. We may also share your information with developers of distributed applications on the UX Network subject to our obtaining your prior consent before doing so;

5.6. Your Personal Data may be transferred to other third-party organisations in certain scenarios:

5.6.1. if we are discussing selling or transferring a part or all of our business – the information may be transferred to prospective purchasers under suitable confidentiality terms;

5.6.2. if we are reorganised or sold, information may be transferred to a buyer who can continue to provide the Services to you;

5.6.3. if we are required to by law, or under any regulatory code or practice we follow, or if we are asked by any public or regulatory authority – for example law enforcement; and

5.6.4. if we are defending a legal claim, your information may be transferred as required in relation to defending such claim.

5.7. Your Personal Data may be shared if it is made anonymous and aggregated, as in such circumstances the information will cease to be Personal Data.

5.8. Your information will not be sold, exchanged or shared with any third parties without your consent, except to provide Services or as required by law.

5.9. Asynq's third-party service providers are contractually bound to protect and use such information only for the purposes for which it was disclosed, except as otherwise required or permitted by law. We ensure that such third parties will be bound by terms complying with DP Law.

Disclosures to Legal Authorities

5.10. We may share your Personal Data with law enforcement, data protection authorities, government officials and other authorities when:

5.10.1. compelled by court order or other legal procedure;

5.10.2. disclosure is necessary to report suspected illegal activity; or

5.10.3. disclosure is necessary to investigate violations of this Privacy Policy, the TARA, the KYC Requirements or Portal Terms.

International Transfers of Personal Data

5.11. We store and process your Personal Data in data centres around the world, where Asynq facilities or service providers are located. As such, we may transfer your Personal Data outside of the European Union. Some of the countries to which your Personal Data may be transferred to for these purposes that are located outside the EU do not benefit from the adequacy decision issued by the EU Commission regarding protection afforded to Personal Data in that country. Details of these specific countries can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

Such transfers are undertaken in accordance with our legal and regulatory obligations, and appropriate safeguards under DP Law will be implemented, such as standard data protection clauses, with data recipients or processors approved by competent authorities. A copy may be requested at the address set out in the Contact Us section.

6. YOUR STATUTORY RIGHTS

6.1. You have certain rights concerning your Personal Data under DP Law, as mentioned below, and can exercise them by contacting us at info@asynq.one.

6.2. **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 DP Law, that before the information is delivered, you specify the information or processing activities to which your request relates.

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

6.4. **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.

6.5. **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.

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

6.7. **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.

6.8. **Automated decisions**: you may contest any automated decision made about you where this has a legally or similarly significant effect and ask for it to be reconsidered.

6.9. You also have a right to lodge a complaint with a supervisory authority, in particular in the Member State of the European Union where you are habitually resident or where an alleged infringement of DP Law has taken place. In the UK, you can make a complaint to the Information Commissioner's Office (Tel: 0044 1625 545 700 or at www.ico.org.uk).

7. RESIDENTS OF THE STATE OF CALIFORNIA (USA)

7.1. Pursuant to the California Consumer Privacy Act of 2018 ("**CCPA**"), California residents have certain rights in relation to their personal information, subject to limited exceptions. For personal information collected by us during the preceding 12 months that is not otherwise subject to an exception, California residents have the right to access and delete their personal information.

7.2. Asynq will not discriminate against any customer that asserts their rights under the CCPA. We will not: (1) deny you goods or services; (2) charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties; (3) provide you a different level of qualify of goods or services; or (4) suggest that you may receive a different price or rate for goods or services or a different level of quality of goods or services.

7.3. If you are a California resident, you have the right to request certain information from us regarding our information-sharing practices with third parties for direct marketing purposes. To the extent that we share your personal information for direct marketing purposes, you may receive the following information: (1) the categories of information and sources of information that we disclosed to third parties for direct marketing purposes during the preceding year; and (2) the names and address information of third parties that received such information, or if the nature of their business cannot be determined from the name, the examples of the products or services marketed.

7.4. To the extent that Asynq sells your personal information to third parties, you also have the right to request that we disclose to you: (i) the categories of your personal information that we sold, and (ii) the categories of third parties to whom your personal information was sold. You also have the right to direct us not to sell your personal information.

7.5. California residents may also designate an authorized agent to make a request to access or delete on your behalf. Your authorized agent must submit proof that you have provided them with power of attorney pursuant to Probate Code sections 4000 through 4465. We may deny a request from a purported authorized agent who does not provide proof of authorization to act on your behalf.

7.6. If you are a California resident, you may exercise your rights by contacting us at the addresses and numbers provided below.

8. SECURITY OF PERSONAL DATA

8.1. We use a variety of security measures to ensure the confidentiality of your Personal Data, and to protect your Personal Data from loss, theft, unauthorised access, misuse, alteration or destruction. These security measures include, but are not limited to:

8.1.1. password protected directories and databases;

8.1.2. Secure Sockets Layered (SSL) technology to ensure that your information is fully encrypted and transmitted online securely; and

8.1.3. PCI Scanning to actively protect our servers from hackers and other vulnerabilities.

8.2. All financially sensitive and/or credit information is transmitted via SSL technology and encrypted in our database. Only authorised Asynq personnel are permitted access to your Personal Data, and these personnel are required to treat the information as highly confidential. The security measures will be reviewed regularly in light of new and relevant legal and technical developments.

8.3. We do not ask for financial or payment information, such as your credit card number, passcode, Account number or pin number, in an e-mail, text or any other form communication that we use to contact you. Please always check that any website on which you are asked for financial or payment information in relation to our reservations or Services is operated by Asynq. If you do receive a suspicious request, do not provide your information and report it by contacting one of our service representatives as set in this Privacy Policy.

8.4. You are responsible for keeping your Account login details safe and secure. Do not share those with anyone. If there is an unauthorised use or any other breach of security involving your information, you must notify us as soon as possible (see Contact Us).

9. RETENTION OF PERSONAL DATA

9.1. We retain Personal Data for as long as necessary to fulfil purposes described in this Privacy Policy, subject to our own legal and regulatory obligations. The criteria we may use to determine the retention period for certain categories of data include:

9.1.1. how long you have been an Account holder;

9.1.2. whether there are contractual or legal obligations that exist that require us to retain the data for a certain period of time;

9.1.3. whether there is any ongoing legal or financial claim that relates to your relationship with us;

9.1.4. whether any applicable law, statute or regulation allows for a specific retention period; and

9.1.5. what the expectation for retention was at the time the data was provided to us.

9.2. In accordance with our record-keeping obligations, we will retain Account and other Personal Data for at least five years (in some cases up to ten years, as required by applicable law) after an Account is closed.

10. UPDATES TO THIS PRIVACY POLICY

10.1. This Privacy Policy was last revised on 27 July 2020. We may change this Privacy Policy from time to time, so it is advisable to review it frequently. Changes to this Privacy Policy will be announced on the Portal or through similar means for a reasonable length of time prior to and following the change taking effect.

11. CONTACT US

11.1. Please contact us with questions, comments or concerns regarding our Privacy Policy and/or practices at info@asynq.one.