Tools for Humanity Orb App and Operating Partner Privacy Notice

Name and contact data of the data controller	Tools for Humanity Corp. 548 Market Street, PMB 49951 San Francisco, CA 94104-5401 USA Hereinafter referred to as “us”, “we”, “company”, “TFH”
Purposes and legal grounds of data processing	This notice applies to the business owners and representatives of companies we collaborate with to mechanically and physically operate the Orbs (“Orb Operators”) and their team members (“Field Staff”, together with Orb Operators referred to as “Operating Partners”). We process Orb Operators’ personal data to administer, fulfill and evaluate our business relationship with Orb Operators and their companies. The legal basis of this processing is performance of contract. We process Operating Partners’ personal data to determine their compensation based on the operator rating that provides an incentive for responsible behavior as an Operating Partner. The legal basis of this processing is performance of contract. We process personal data to determine whether we enter into a business relationship with Orb Operators and their companies. This includes a Know Your Customer (KYC) procedure to comply with anti-money-laundering and anti-terrorist-financing laws and to prevent fraud. Our legal basis for this processing is that it is necessary to comply with our legal obligations and our legitimate interest to make an informed decision about the companies and individuals we collaborate with. We process Operating Partners’ personal data to provide the Orb App that allows Operating Partners to administer their relationship with us and operate the Orbs. The legal basis for this processing is performance of contract. We process Operating Partners’ personal data to ensure the Orb App is functioning securely and to improve the Orb App. The legal basis for this processing is legitimate interests, namely the interest to provide a secure and well functioning Orb App. We process Operating Partners’ personal data to ensure trust and safety and prevent fraud. The legal basis for this processing is legitimate interests, namely the interest to ensure trust and safety and to prevent fraud.
Categories of recipients	Externally we only share data under contractual safeguards and only with selected service providers that ensure the security and protection of the data: ● **With vendors and service providers outside of our organization:** We only disclose data to service providers whose services we rely on in order to process the data and provide our Services to you. We only disclose data with identity verification vendors if required by Law (i.e., know-your-customer requirements). ● The categories of such service providers are:

- Cloud service providers (all data types)
- SaaS providers; we use SaaS products in the following categories:
    - Database and infrastructure management
    - Data security
    - Recruiting
    - Communication
    - Surveys
    - KYC/KYB i.e. checking official documents
    - Data subject request management
    - Technical support
    - User support
- External experts
    - Specialist software developers
    - Legal specialists
    - Tax advisors
- Banks
- Labeling service providers (only under special safeguards)
- Background check services for applicants and Orb Operators
- **With law enforcement, officials, or other third parties:** We may disclose your data in order to comply with applicable laws and respond to mandatory legal demands. We will carefully consider each request to determine whether the request complies with the law and, where appropriate, we may challenge invalid, overbroad, or unlawful requests. We may share personal data with police and other government authorities where we reasonably believe it to be necessary to comply with law, regulation or other legal process or obligation.
- We may share your personal information if we believe that your actions are inconsistent with our User Terms, if we believe that you have violated the law, or if we believe it is necessary to protect our rights, property, and safety, our users, the public, or others.
- We may share your personal information with our lawyers and other professional advisors where necessary to obtain advice or otherwise protect and manage our business interests.
- We may share your personal information in connection with, or during negotiations concerning, any merger, sale of company assets, financing, or acquisition of all or a portion of our business by another company.
- Data, including your personal information, may be shared between and among our current and future parents, affiliates, and subsidiaries and other companies under common control and ownership.

	• We may share your personal information with your consent or at your direction.
Personal Information Collection, disclosing which personal information you collect	For the purposes of performing and administering the contractual relationship with Operating Partners we collect and process the following information • Basic contact information (such as name, postal or email address, phone number, both current and previous) • Demographic data (such as your birthday) • Contract details • Wallet addresses and bank accounts For the purposes of our KYC procedure of Orb Operators we collect and process the following information: • Basic contact information (such as name, postal or email address, phone number, both current and previous) • Demographic data (such as your birthday) • Government document and identifiers • Audio, video and photos of you • Files you upload • Device information (such as IP address) • Third party account information • Metadata like geolocation data and timestamp For the purpose of evaluating and monitoring Operating Partners' performance we collect and process the following information: • Number of sign-ups • Aggregated quality evaluation of sign-ups through several signals that include user engagement and trust and safety complaints For the purpose of providing the Orb App for Operating Partners and ensuring trust and safety, prevent fraud and improving the Orb App we collect and process the following information from Operating Partners "Orb App User Data" from Operating Partners: • User profile including all the data you chose to provide in this context • Phone number • E-Mail address • Name

	• Aggregated data of user sign-ups • Balance • Wallet address • Relation to team/Orb Operator (if applicable) "Orb App Metadata" from Operating Partners: • Device data • IP address • Usage events • Geolocation of Orb in case of Orb activation
Retention period	We delete personal data pertaining to the contract and to the compensation related to tax purposes for 10 years and data processed as part of our KYC procedure 5 years after the termination of the business relationship. Other data from the business relationship is deleted three years after termination of the contract. In some cases, we might be required by law to retain such personal data for longer. We retain Orb App User Data for one year. In some cases, we might be required by law to retain such personal data for longer. We retain Orb App Metadata for one year. In some cases, we might be required by law to retain such personal data for longer.
Subjects' rights	Under the applicable data protection laws you might have the following rights/ You can make use of your data subject rights by sending an e-mail to the following email address or postal address: dpo@worldcoin.org • You have the right to obtain from us at any time upon request information about the personal data we process concerning you. • You have the right to demand that we immediately correct the personal data concerning you if it is incorrect. • You have the right to demand that we delete the personal data concerning you. These prerequisites provide in particular for a right to erasure if the personal data are no longer necessary for the purposes for which they were collected or otherwise processed, as well as in cases of unlawful processing, the existence of an objection or the existence of an obligation to erase under Union law or the law of the Member State to which we are subject. • You have the right to demand that we restrict processing. • You have the right to receive from us the personal data concerning you that you have provided to us in a structured, commonly used, machine-readable format. • You have the right to object at any time, on grounds relating to your particular situation, to the processing of personal data concerning you which is carried out

	based on legitimate interests. • You have the right to contact the competent supervisory authority in the event of complaints about the data processing carried out by the controller. The responsible supervisory authority is: The Bavarian Data Protection Authority (“BayLDA”). • If the processing of personal data is based on your consent, you are entitled to revoke your consent to the use of your personal data at any time with effect for the future, whereby the revocation is just as easy to declare as the consent itself. We will not discriminate against you for exercising your data subject rights.
Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data	For Orb Operators participating in the KYC process is necessary. We are obliged to verify your identity prior to establishing a business relationship with you. To enable us to fulfill this legal obligation, you must provide us with the necessary information and documents and notify us immediately of any relevant changes that arise in the course of the business relationship. If you do not provide us the necessary information and documents, we may not enter into or continue the business relationship requested by you. For Operating Partners participating in the Orb App is necessary in order to be able to operate the Orbs.
Automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject	Please note that processing of your personal data may include automated decision-making including profiling. We may apply automated decision-making including profiling for onboarding, fraud prevention and verification purposes. We may use verification services provided by an external vendor during the onboarding process, including validation of KYC documentation, and information checking in national registers. The automated decision-making is necessary for entering into a business relationship with us.
Third country transfers	We are in the USA and some of our service providers are established in the USA while others are located in the European Union. For transferring personal data to the USA, we rely on appropriate safeguards as provided by the Standard Contractual Clauses adopted by the European Commission. The country in which your data is transferred, stored, or processed may not have the same data protection laws as the country in which you initially provided the data. We adhere to the principles stated in the European Union’s General Data Protection Regulation (GDPR), even when not required. For example, we only share data with data processors outside of the EEA if such a transfer is lawful and if we are confident that the data processor will protect your data as required under applicable laws and, further, in accordance with our standards.

	Below is a list of possible risks that may arise if we transfer your data. Below we also summarize how we mitigate the respective risks. ● While we do what we can to ensure that our subcontractors are contractually obligated to adequately protect your data, these subcontractors may not be subject to the data privacy law of your country. If the subcontractors were to illegally process your data without authorization, then it may be difficult to assert your privacy rights against that subcontractor. We mitigate this risk as we close strict data processing agreements with our subcontractors that oblige them to protect the data as required under GDPR and to fulfill data subjects' requests. ● It's possible that the data privacy law in your country is inconsistent with the data privacy laws in the U.S. or in the E.U. We always try to adhere to the highest standard of data protection we are subject to. ● It may be possible that your data will be subject to governmental access of officials and authorities. In those cases we have committed ourselves to challenge any invalid, overbroad, or unlawful governmental request to access in court. We further use advanced encryption to hinder unauthorized access. Please note that this list contains examples, but may not include all possible risks to you.
Sharing and Selling of Personal Information	We are not selling personal data.