Tools for Humanity Privacy Policy

This Privacy Policy explains how Tools for Humanity Corporation ("We", "TFH") processes your data when you use World App, our websites and services (collectively, our "Services"). We've tried to keep this policy simple, and **We never sell your personal information**.

If you use World App or an Orb built by TFH to verify your World ID, the first section of this Privacy Policy is relevant to you. Other companies can build apps ("Compatible Applications") and or Orbs to enable people to create, store, verify, or use their World ID.

World ID and Orb Verification

You can create and store a World ID by using a Compatible Application. Once you have created and stored your World ID, you can choose to verify your World ID.

Creating a World ID

You start by installing a Compatible Application to your phone. The Compatible Application will automatically create a random number, your World ID Secret. It lives on your mobile device and is never revealed to anyone.

Verifying a World ID

To verify your World ID, you then can make an appointment with an Orb. The Orb will: photograph your face and eyes; analyze the images to confirm you're a unique human; generate an iris code; anonymize that iris code; encrypt the photos, iris code, and anonymized data and send them to your phone; and permanently delete all of that data from the Orb. Learn more about the Orb.

Humanness

First, neural networks on the Orb assess the photos to determine whether the person in the photos is a living human to block deepfake images and photos on a screen that are trying to defraud the Orb.

Uniqueness

Second, we check that you have not already verified a World ID before – ensuring that you are unique. For that purpose, the Orb generates abstractions of the eye photos to create an iris code. An iris code is a series of 12,800 zeros and ones that abstract the details of the eye. The iris code is then anonymized using homomorphic encryption through Shamir Secret Sharing in a Multi-Party Computation—this is called Anonymous Multi Party Computation or AMPC. Learn more about AMPC. After anonymization, uniqueness is verified by cryptographically comparing the AMPC fragments against large databases of other AMPC fragments, that cannot be linked to an individual, to see whether the new AMPC fragments are in fact unique.

Custody

The photos, the iris code, and the AMPC fragments are cryptographically signed and encrypted so they can be securely transmitted and stored on your phone. The data is then permanently deleted from the Orb. This means you alone have a copy of

your personal data. Learn more about Personal Custody. You can use the photos on your phone for face authentication. Face authentication matches a selfie of your face to the cryptographically signed photos taken by the Orb to ensure that you are the rightful owner of the World ID. Face authentication also takes place fully on your phone. Learn more about Face Authentication.

How is the data anonymized?

The encryption into AMPC fragments is random—even if you attempt to verify twice, the fragments will be completely different each time. The special method by which AMPC fragments are calculated allows that they can still be used to determine uniqueness, but nothing else. Storing the AMPC fragments with universities and other parties that enjoy public trust ensures that AMPC fragments will not be recombined or used for any other purpose besides the uniqueness test. This way, no personal data is retained or accessible by any World protocol contributor or participant, or any third party.

Using World ID

If your Orb verification was successful, the hash of your World ID secret (a random number) is added to the public list of verified World ID hashes without ever learning who you are, or what data was collected on the Orb. When you use your World ID, you prove from your phone that you have the World ID secret to one of the hashes in the Hash Tree without revealing which one. A Zero Knowledge Proof (ZKP) ensures that you don't reveal which of the hashes you are relying on. Instead, the ZKP creates a nullifier hash for the specific action that can be best described as an action specific, disposable World ID. This allows you to use World ID anonymously. This means if you log into two different services using your World ID and those services try to identify you by sharing your nullifier hash, they cannot identify you. This does not solve or stop them identifying you through other means historically used by online platforms, but over time could help address the problem of online tracking. Learn more about ZKPs.

Personal Data We Collect And Use

We collect your personal data when you provide it to us and when you use our Services. In limited cases, We also receive personal data from third parties. As explained further below, you can access, correct, or delete your personal data at any time.

Personal data you provide us

Data listed in this section is optional to provide. You can change your mind and modify or delete it at any time in the settings of World App.

- You can add your **phone number** to your World App account. This helps your contacts to find you and interact with you. You can also use your phone number to restore backups and rely on our referral system (see our partnership referrals).

- You can sync your **contacts** with World App. This allows you to see which of your contacts have added their phone number to World App so that you can more easily connect and interact with them. We do not store your contacts.

- You can create a **username**, which you can change at any time. Your username is only linked to your wallet and not to your World ID.

- You can share your **geo-location** with us to find an Orb near you and help us understand where We should make Orbs available in the future.

- You will be asked to enter your **date of birth**. Your date of birth is not retained or stored and is only used on your device to determine if you meet the minimum age requirements to use the Services.

- If you contact us, for example for help or support, We will process **messages and communication** with you which can contain your personal data. If you provide feedback through surveys, We will use your feedback to improve our services.

- If you are using World Chat **We cannot see or access your chat messages**. The messages and related metadata are end-to-end encrypted and We cannot decrypt or otherwise access them. We only route the encrypted messages through our server from the sender of a message to its recipient.

- You can choose to allow us to analyze information about **your interactions with World App** to help us find bugs and improve our products.

- You can choose to provide your data to **improve World ID for everyone**. To ensure that World ID is secure, reliable, and inclusive, the models powering it require training data from a diverse population. You can optionally share your Orb photos and Face Authentication photos to help train those models.

- You can add **Credentials** like a passport to your World App. We will check the validity of your credential, confirm your face matches the photograph on the credential and then store your credential's data securely on your device. We never have access to the personal information contained on your credential.

Information We collect when you use our Services

- When you use World App We collect information about your connection, such as your **IP address**, browser type, and related data to provide our Services and tailor them to the country you are in. We collect further **device metadata** like your screen resolution, operating system, carrier, language, memory, apps installed, battery level, and device number to ensure your app functions well on your device and complies with our Terms and Conditions. We also use this information to detect and prevent fraud.

- We collect further information about your **interactions with World App** to ensure it works the way you expect (*e.g.*, store your settings and your verification level to show you the appropriate interface).

- The first time you open World App on your phone it randomly generates a crypto wallet including a **wallet address** for you. We process that wallet address to enable transactions involving your wallet. The corresponding private key to the wallet is only stored on your device and We never have access to it.

- To comply with legal obligations and to provide an interface for blockchain transactions, we collect up to date copies of the state of **public blockchains** which can contain your previous, public transactions.

- Our websites use **Cookies**. Cookies are small text files stored on your device that online services use to identify your device and/or preferences. We use functional Cookies to ensure a functioning website experience to you, and optional Cookies to analyze and improve how our websites are used. For a full list of the Cookies and your options to reject non-essential Cookies please see our Cookie Policy.

Information We may receive from third parties

- If you need to use our support portal to verify your age, We request confirmation from a third party that has independently verified your age that you are at least the **age of majority** in your country. We do not receive any other information from this third party.

- To prevent fraud and illicit activities on our Services, We receive information from third-party providers about devices and blockchain wallets linked to potential fraud and or illicit activity.

Sharing Personal Data

Within TFH, only team members who need to access or see personal data to perform their tasks can do so, and We have strict access controls in place to ensure this. We only outsource data processing to trusted and secure vendors and service providers. These service

providers include certified cloud service providers, software as a service providers, and IT security firms. Please find here the complete list of our outsourced processors.

We may share your data to comply with legal requirements or respond to lawful requests from Law Enforcement authorities. If your actions violate our Terms and Conditions, or pose a risk to our or other's rights, we may give your information to relevant authorities. We will share your personal information with your consent or at your direction.

How Long We Keep Personal Data

Generally, We retain your personal data as follows:

- personal data you provide us, We retain for as long as you use our Services, or until you decide to modify or delete it;

- information We collect when you use our Services, We keep for no longer than two years. Your previous interactions with World App (that we require to keep the app functioning), We retain for the duration of your use of Services, or until you delete your account;

- wallet data is permanently published on the public blockchain, of which We frequently retrieve an updated copy; and

- information We may receive from third parties (typically to prevent fraud and keep you and others safe while using our Services), We keep for one year unless you have violated our Terms then We keep it for five years.

If required by law, We will retain your personal data as necessary to comply with our legal and regulatory obligations, including fraud monitoring, detection, and prevention, as well as tax, accounting, and financial reporting obligations.

For detailed information regarding the specific legal grounds and purposes for our data processing activities, please refer to the chart below, which explains the data We collect, what We use it for, and how long it is retained.

Your Rights

Your data is your data, and We believe you should be able to easily exercise your rights at any time. When you use our Services you can always:

- learn more about the data processing through support materials here or contacting our Data Protection Officer here;

- access and get a copy of your personal data here;

- correct any your personal data in the Settings of World App;

- delete your personal data by going to settings, clicking on Privacy & Legal and selecting to delete optional data or delete your full account; and

- revoke your consent to data processing based on consent or object to processing based on legitimate interests including the demand to restrict processing by going to your settings in World App under Privacy & Legal.

You can exercise these rights in World App by clicking on Privacy & Legal under settings; for more information on deletion, see this help center article.

General

We comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. We have certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of

personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DP. We have certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit Data privacy framework website.

You must be at least the age of majority in your country (and a minimum of 18 years old) to use our Services. We take the protection of minors seriously—if you believe someone under 18 years of age is using our Services, please contact us immediately via our Privacy Portal or the channels above.

We can update this Privacy Policy any time, but if the changes affect your rights we'll notify you in advance. If you use our Services after that, you accept the updated Privacy Policy.

How To Contact Us

If you have questions about this Privacy Policy or other data related questions, you can contact us at any time. You can always contact our Office of Data Protection and Data Protection Officer, Julian Moore, at dpo@toolsforhumanity.com or by sending a letter to: DPO, Tools For Humanity Corporation, 650 7th St, San Francisco, CA 94103, USA.

If you live in the United States or any other country outside of the European Union, EFTA States, or the United Kingdom, the data controller responsible for your personal data is Tools For Humanity Corporation, with an address of 650 7th St, San Francisco, CA 94103, USA.

If you live in the European Union, EFTA States, or the United Kingdom, the data controller responsible for your personal data is Tools for Humanity GmbH, with an address of August-Everding-Straße 25, 81671 München, Germany.

If you wish to raise a concern about data practices, you have the right to do so with your local supervisory authority or TFH GmbH's lead supervisory authority, the Bavarian Data Protection Authority ("BayLDA") using the contact details listed on their website.

ANNEX – Legal bases/purposes for Tools for Humanity data processing activities

TFHPS20250801