DISCLAIMER

This Privacy Notice is for Research and Development purposes only, it is not applicable to World App users and does not reflect data processing in the context of verifying your World ID with an Orb.

To ensure that World ID is as reliable and inclusive as possible, the neural networks powering it require to be trained with data from a diverse population. To collect that training data the World contributor Tools for Humanity collects this data transparently in dedicated data collection campaigns for which the following privacy notice applies. You can delete your full data at any time as described in the section on data subject rights.

Name and contact data of the data controller	**Tools for Humanity Corp. ("TFH", "us", "we")** 548 Market Street, PMB 49951, San Francisco, CA 94104, USA

Categories of Data Collected	Depending on the data collection campaign we may collect the following categories data with your consent:
	
	 • **If you take part in Orb testing or data collection we collect the following information**
	
	   ○ **Image Data:** Images of your irises and eyes captured in visible and near-infrared spectrum, as well as images of your face, including 3D depth images.
	
	   ○ **Derivatives:** We create abstractions of the Image Data using advanced algorithms and neural networks to enable machine comparisons and interactions.
	
	 • **If you take part in credentials ("NFC ID") testing or data collection we collect the following information:**
	
	   ○ We collect data from the NFC chip of your passport, including your full name, date and place of birth, passport number, issuance and expiry dates, passport picture, and any other relevant data.
	
	   ○ We also collect the selfie (i.e. the photo you took of your face) to match the passport photo, your gender and ethnicity.
	
	 • **If you take part in credentials ("NFC ID") testing or data collection via a third party platform like clickworker (mini-job campaign) we collect the following information:**
	
	   ○ We collect your passport photo (face image).
	
	   ○ We also collect the selfie (i.e. the photo you took of your face) to match the passport photo, your gender and ethnicity.
	
	   ○ We ask individuals to share their childhood photos to help improve our age estimation models. These models are intended to support our efforts in ensuring that only adults access our services and to verify their uniqueness.
	
	 • **Video recordings**: depending on the research or testing initiative, we might collect, store and analyze a video of your Orb verification if we asked you and you explicitly agreed to it.
	
	 • To ensure that our products are secure, reliable, and inclusive, the models powering it require

training data from a diverse population. To prevent algorithmic bias, i.e., to ensure that we train our models with balanced data that is representative of the world's population, we may ask which **gender and ethnicity best describes your appearance**.

- If the testing is conducted with your data collection app the following data may have been collected:

    - **Administrative Information via our Data Management App**: email address, first name, last name, the first letter of both parents' first names (for randomness), date of birth, and timestamps related to your consent and feedback you provide to us. This data is only collected if you actively enter it in the application.

    - **App Metadata:** screen resolution, operating system, device used, hashed IP address, and timestamps.

Purposes and legal grounds of data processing	In the context of this processing we collect the personal information described above for the following purposes: - To perform product testing, to enhance user experience, ensure product usability, and maintain product security. - To develop and improve our (Data Management App) products. - To train neural networks and AI models which includes to label data to promote algorithmic fairness by considering perceived gender, age range, and skin color. The legal basis for processing your data is your explicit consent, which allows us to utilize this information responsibly and ethically in our research and development initiatives.
Data Security	- Access control: Your data is stored in a secure server environment with limited access, meaning that only authorized personnel can view or handle it. - Encryption: Your data is encrypted at rest and in transit. - Data Management: You can easily manage your personal data through our web based Data Management Application ('Data Management App').

Categories of recipients	We do not share the images or derivatives of the images with anyone not working on the World Project. Only the following categories of recipients may receive your data to enable the above listed purpose of processing.
	
	- Subsidiaries
	
	- Internal teams
	
	    - We only share your data with team members who need to have access to the data to perform their tasks (access on a need to know basis)
	
	- Third party service providers. In this context we use the following categories of processors to enable the data processing:
	
	    - Cloud service providers
	
	    - Communication tools

	○ IT service provider to provide the interface for testing and data collection
Retention period	We retain the NFC Data for a maximum of 3 years We retain video recordings for a maximum of 2 years. We commit to delete all Image Data and Derivatives collected for our data collection efforts after a maximum of ten (10) years after collection. We store your Administrative Information for as long as we store the corresponding data. In any case, we will delete the NFC Data, Image Data or any other type of data collected for the purpose of this Notice upon your request.
Subjects' rights	Under the applicable data protection laws you have the following rights: ● to information about the personal data we process ● to access to and a copy of the personal data ● to correction of personal data ● to deletion of personal data ● to demand that we restrict processing ● to object to personal data processing based on legitimate interests ● to contact the competent supervisory authority ○ The responsible supervisory authority under the EU's General Data Protection Regulation ("GDPR") is: The Bavarian Data Protection Authority ("BayLDA"). ● Right to revoke your consent to the use of your personal data You can exercise these rights by contacting: contribute@toolsforhumanity.com or sending a letter addressed to "DPO", Tools For Humanity Corporation, 548 Market Street, PMB 49951, San Francisco, CA 94104 USA. If you withdraw your consent, then we will no longer use your data for the purposes stated above. If the data was collected in our data collection application you can also delete your data by clicking the button "request full data deletion" in the settings of the data collection app.
Necessity	You do not need to provide your personal data or agree to video recording in order to participate in product tests. You can also share your feedback directly with us.
Third country transfers (GDPR), under the CCPA already who you share the personal data with	Data is stored and processed in the USA and EU. TFH complies 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. Further information can be found in TFH's general privacy notice available under www.toolsforhumanity.com

Sharing and Selling of Personal Information	We are not selling personal data.

PRANDD20250320