

Test Data Collection Consent Form (NFC)

NOTE: THIS ONLY PERTAINS TO TESTING AND TRAINING WHICH IS DECOUPLED FROM REGULAR (ORB) OPERATIONS.

I agree to the following data collection:

Tools for Humanity Corp and Tools for Humanity GmbH will collect my machine readable passport data in the NFC chip, a photo of my passport and a selfie for the purpose of testing and developing software in the context of secure digital identity with that data. You can freely revoke your consent at any time (e.g. by clicking a button in the app).

The details of the data collection will be explained in great detail below.

1. Background.

1.1 The Purpose.

We develop new technologies in the context of Proof of Personhood (the proof that someone is a unique human being without disclosing which one) and decentralized digital identity (I can prove who I am i.e. by name). For this context we ask you for your data to test our products and to train our neural networks. We call this Test Data Collection.

For this purpose we have developed a web application for computers and phones alike that allows you to manage your data (Data Management App). Our Data Management App implements state-of-the-art encryption techniques and follows strict privacy protocols to safeguard your personal information. Your data will be stored in a secure server environment with restricted access, ensuring that only authorized personnel can handle it.

We have also developed a smartphone application that allows us to test certain functionalities and features in the field of Proof of Personhood and decentralized digital identity ("Test App"). Our Test App implements state-of-the-art encryption techniques and follows strict privacy protocols to safeguard your personal information. Your data will be stored in a secure server environment with restricted access, ensuring that only authorized personnel can handle it.

1.2. The Controllers

The joint data controllers are:

- Tools for Humanity Corporation, 548 Market Street, PMB 49951, San Francisco, CA 94104 USA, and
- Tools for Humanity GmbH, Allee am Röthelheimpark 41, 91052 Erlangen, Germany

The details of the joint controllership arrangement are as follows: Tools for Humanity Corporation is primarily responsible for developing, operating, and supporting the Services, including responding to data subject requests and complying with any statutory obligations. Tools for Humanity Corporation maintains the contracts the most service providers, particularly in the context of cloud hosting services i.e. Tools for Humanity Corporation is responsible for the storage and security of the data in the context of this test data collection.

Tools for Humanity GmbH is primarily responsible for developing and training the algorithms, building and managing the data flows from the Orb to our servers. This test data collection is operationally overseen by Tools for Humanity GmbH.

To you, as the test user, both entities act as a single entity. Users can contact either entity for any processing activity. In the relation to the user both entities declare themselves equally responsible for any activity.

2. Data Processing.

2.1 Data We Collect

With your consent, we collect the data contained on your passport's NFC chip. The NFC chip is a computer readable piece of hardware integrated into your passport. It allows modern smartphones to read the information contained therein. This data on your NFC chip ("NFC Data") might include:

- Your full name
- Your date of birth and your place of birth
- Your passport's number, date of issuance and of expiry
- Your passport picture
- Other data contained on your passport (as not all passports contain the same information on the NFC chip)
- Metadata

With your consent, we will also collect a photo of your passport's front page and a selfie of you to match that against the photo of your passport ("Passport Authentication Data")

2.2 What We Do with This Data.

We use Data from the Test App and the Data Management App only for the purpose of providing the Data Management App and to administer our data collection e.g. by contacting you if you have questions about the project, to explain to you what we are doing with your data or to contact you in connection with our project. The legal basis for this is legitimate interest. The legitimate interest pursued is providing an infrastructure for data donations and data collection where users can easily administer their data and withdraw their consent.

With your consent, we use the NFC Data and Passport Authentication Data for the following purposes:

1. Store the NFC Data and Passport Authentication Data;
2. Send the NFC Data and Passport Authentication Data to our team in the European Union;
3. Use the NFC Data and Passport Authentication Data to continue developing and improving the software. In detail this means:
 - a. Analyze the data for particularities of local passports' NFC Data and Passport Authentication Data
 - b. Find bugs and errors in our software
 - c. Run tests for our software
 - d. Experiments that help ensuring that NFC Data and Passport Authentication Data can be used securely in the context of Proof of Personhood and decentralized identity

We will never sell your data. We will also not use any data listed in this form to track you or to advertise third parties' products to you.

2.3 Whom We Share the Data With

When we share your data outside of TFH, we will always:

- Share it in a secure way;
- Take steps to ensure that it is handled in a manner that is consistent with our commitment to your privacy; and
- Prohibit other companies from using it for their own purposes.

If you enable data custody we do share your data in these limited ways:

- **With Worldcoin:** We may disclose data with the Worldcoin Foundation or a subsequent non-profit organization responsible for promoting and furthering the mission of the Worldcoin project.
- **Within TFH:** We only disclose data to our team members who require access in order to perform their tasks and duties. We only disclose as much data as is needed to perform specific tasks and duties and have a system of strict access control.
- **With vendors and service providers outside of TFH:** 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
 - Data subject request management
 - Technical support
- External experts
 - Specialist software developers
 - Legal specialists
- Labeling service providers

We do not share the images or derivatives of the images with anyone not working on the Worldcoin project

2.4 Retention of Data.

We will retain the NFC Data for a maximum of 12 months. In any case, we will delete the NFC Data upon your request.

2.5 International Data Transfer

We will transfer your data to the European Union. Our legal basis for this are existing mutual adequacy decisions finding the level of data protection in the EU to be equal to the level in the UK.

2.6 Withdrawing your Consent

You can withdraw your consent at any time by contacting us at: contribute@toolsforhumanity.com or by a letter addressed to one of our physical addresses with the subject "DPO request".

You can also delete your data from within the App under the Settings menu. If you withdraw your consent, then we will no longer use your data for the purposes stated above.

3. Statutory rights

To exercise your rights please contact us at contribute@toolsforhumanity.com. The following list explains the most important statutory rights you have regarding your personal data.

- You have the right to obtain from us at any time upon request information about the personal data we process concerning you within the scope of Art. 15 GDPR.
- You have the right to demand that we immediately correct the personal data concerning you if it is incorrect.
- You have the right, under the conditions described in Art. 17 GDPR, 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 in accordance with Art. 18 GDPR.
- 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 in accordance with Art. 20 GDPR.
- 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, inter alia, on the basis of Article 6 (1) sentence 1 lit. f GDPR, in accordance with Article 21 GDPR.
- 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 State Office for Data Protection Supervision (Bayerisches Landesamt für Datenschutz).
- If the processing of personal data is based on your consent, you are entitled under Art. 7 GDPR 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. Please note that the revocation only takes effect for the future. Processing that took place before the revocation is not affected.