Tools for Humanity Privacy Notice

Thank you for choosing to be part of the Worldcoin Community! Worldcoin is an open-source protocol, supported by a global community of developers, individuals, and other contributors.

This Privacy Notice covers the data you provide to us through your use of our websites, applications ("App"), and other services linked to this Privacy Notice (collectively, the "Services"). This Privacy Notice is incorporated into and governed by the User Terms and Conditions ("User Terms"). Tools for Humanity Corporation ("TFH US"), along with its German subsidiary Tools for Humanity GmbH ("TFH Germany"; together, "**TFH**" or "**we**," "**us**"), is contributing to the development and growth of the Worldcoin protocol ("Worldcoin") but is different from the Worldcoin Foundation that controls the Orb related data processing.

1. Controller

We are the data controller of all "World App Data", "Credential Verification Data" and other "Business Data": Tools for Humanity Corporation, 548 Market Street, PMB 49951, San Francisco, CA 94104 USA. TFH is established in the European Union ("**EU**") through Tools for Humanity GmbH.

- "World App Data" means all personal data collected and processed through your use of the World App, as defined further in Section 5 below, except any personal data related to your use of the Worldcoin protocol or the Worldcoin tokens (such as your wallet address and the transactional data, which we do not control).
- Credential Verification Data refers to the data processed when verifying a credential to add it to your self-custodial World ID. This means e.g. reading the NFC chip of your passport to securely store your passport's information on your device. This data is under your control and after verifying the validity of your credential, TFH stores an anonymized fragment of a hash value of a unique cryptographic signature of your credential (e.g. passport) to ensure that each credential can only be added to a World ID once.
- "Business data" means all personal data collected and processed through other means by our company when communicating or any other way working or interacting with us via email, video conferencing or our websites. For data processing in the context of the Orb App please refer to the Orb App Privacy Notice linked in the Orb App. For data processing in the context of dedicated data collection and testing please refer to the respective Collection and Testing Privacy Notice linked in your test app. For processing in the context of our website please refer to our Cookie Policy linked on our website.

2. Updates to this Privacy Notice

We update this Privacy Notice sometimes. If we make major changes, such as how we use your personal information, then we'll let you know via an email or a message in your App.

3. What is in this Privacy Notice?

- How this Privacy Notice differs for children and teens
- The statutory rights you have
- How to contact us about this Privacy Notice

4. Our Commitment to Protecting your Privacy and Data

We are deeply committed to protecting your privacy and securing your data. We recognize that we can only fulfill our mission of distributing our digital tokens fairly to as many people as possible if people trust us, and privacy and data security are central to earning your trust.

Privacy

We have designed our products and services with your privacy in mind. We collect data to improve our product and services. We will always tell you, here in this Privacy Notice or in data consent forms for specific products or services, what data we are collecting, why we are collecting that data, and what we do with it.

Data Security

We have a dedicated team to look after your data and have implemented physical and electronic safeguards that protect your data both in transit and at rest. At the same time, no service can be completely secure. If you have any concerns about your account or your data, please contact us through our Request Portal or write to us at Tools For Humanity Corporation, 548 Market Street, PMB 49951, San Francisco, CA 94104 USA.

5. Information We Collect and Why

5.1 Data You Provide To Us

As a user, you are not required to provide any data to access the App. However, you may need to provide us with certain data in order to use a feature within the Services. The legal grounds for processing in the cases below are the user's consent and the performance of a contract (our commitment to provide the Services). Below is a list of data that you may provide and what we may use the data for:

In the Context of World App:

- **Phone number.** You may choose to enter your phone number to associate it with your account. With your permission, other users may be able to find your account through your phone number. We may require a phone number when you submit a data subject request. The legal basis for processing this data is performance of the Service under the User Terms.
- **Username.** You may link a username to your wallet address and change the username at any time.
- **Date of Birth.** You may disclose your date of birth to ensure compliance with age restriction requirements. We will never store your data of birth but only a checksum of that data and whether you are over 18 years of age or not.
- **Feedback and correspondence from you.** These include any emails, chat messages, or other communications that you send us via email or third-party social media websites. This may include processing email addresses or social media profile names if you seek to communicate with us through such means. We may use a third-party service provider to facilitate surveys about your use of our Services. The legal basis for processing this data is performance of the Service under the User Terms.
- **Address book contacts.** You may provide the App with access to your address book to enable the feature that makes it easy for you to find and interact with other users who may be in your address book. The legal basis for processing this data is the legitimate interest of the subject to be found within the App and the interest of the sharing user to find her contacts in the App.

Please note: You are responsible for ensuring that sharing your contacts' information complies with applicable laws. This may require that you obtain your contacts' permission and you shall not share with TFH any contact details from other people without their explicit consent. You can change your mind and turn off our access to your contacts at any time in your device settings. If you elect to import your device's address book contacts to the App to find out which of your contacts uses our Services or invite them to join you in using our Services, we will periodically sync your contacts' phone numbers to those numbers and corresponding

wallet addresses provided by other users on our servers.

- **Location information**. You may decide to enable a location-based service (such as a feature allowing you to find an Orb Operator near you). Only with your specific consent, we may then collect information about your location through GPS to enable the location based service to show you an Orb near you. You can change your permissions any time in your device's settings. If you are not based in South Korea we may also store your approximate location disassociated from your World App account. We use this data to improve our services particularly but not limited to the selection of Orb locations.
- **P2P Marketplace**. If you use the P2P Marketplace Services (where available) that allow you to purchase digital tokens from other users, then we may collect additional information such as your wallet address, your contact information (i.e. your phone number), and your account number associated with the transaction (such as your M-PESA number). We log the transaction data as part of providing the P2P Marketplace Services. We may also collect additional information to comply with applicable KYC requirements.
- **Device metadata.** If you are using the App we are collecting metadata from your device to ensure that the App is functioning properly and that you are not infringing our Terms and Conditions. This includes collecting device identifiers and IP addresses.
- **Device World ID data.** We also process your device metadata to calculate a unique device fingerprint. The hash of this fingerprint serves as the signal that proves the uniqueness for your with a device World ID.

In the context of Business Data processing:

- **First and last name.** We may process your first and last name to pursue the legitimate interest of maintaining and administering a business relationship with you.
- **Email address.** You may also provide your email to subscribe to our mailing list to stay up-to-date with the Worldcoin project. We may require your email when you submit a data subject request. We may process your email address to pursue the legitimate interest of maintaining and administering a business relationship with you.
- **Phone number.** We may process your phone number to pursue the legitimate interest of maintaining and administering a business relationship with you.
- **Enterprise Data**. If you have a business relationship with us (such as if you are an Orb Operator or a supplier), then we may require information such as names, mailing address, email, phone number, wallet address, and other documentation (such as your government ID) as part of furthering that business relationship and to satisfy our know-your-customers obligations. We may use third-party services, such as Onfido, to help us collect and review the information and documentation above to satisfy the know-your-customers obligations.
- **Application data**. If you want to work for us you have to send us your application that includes your cover letter and CV as well as the personal information you wish to disclose.

You can find the legal base for processing for each of the data processing activities above detailed in **ANNEX I – Legal grounds for Tools for Humanity data processing activities** at the end of this privacy notice.

5.2 Data We Collect From Third-Party Sources

From time to time, we may obtain information about you from the following third-party sources:

- **Blockchain Data**. We may analyze public blockchain data to ensure parties utilizing our Services are not engaged in illegal or prohibited activity under the User Terms, and to analyze transaction trends for research and development purposes.
- **Identity Verification Services**. We may obtain information from third-party services using your data to verify your identity if required by law (such as applicable know-your-customer requirements). To clarify, we do **not** use your biometric data when we verify your identity as required by law.
- **Talent data bases**. We may collect data from various sources to make job offers to talented individuals.

5.3 Data We Collect Automatically

If permitted under applicable law, we may collect certain types of data automatically when you interact with our Services. This information helps us address customer support issues, improve the performance of the Services, provide you with a streamlined and personalized experience, and secure your Account credentials. Information collected automatically includes:

- **Online Identifiers:** Geo-location and tracking details (see above), computer or mobile phone operating system, web browser name and version, and IP addresses. In very limited cases these data are also fed into our fraud and illicit financial flow detection. They also serve to provide a stable and fraud-free experience of our software.
- **Usage Data:** Authentication data, security questions, and other data collected via cookies and similar technologies.
- **Cookies**: small data files stored on your hard drive or in-device memory that help us improve our Services and your experience, see which areas and features of our Services are popular, and count visits. For the legal basis processing those data please refer to our Cookie Policy where we explain the different kinds of cookies we are using.

Similarly, the App gathers information for troubleshooting and improvement. We use third-party services, such as Segment.io or PostHog, to view aggregated information about end user usage and interactions. Where possible, we take steps to minimize or mask the information sent to third parties (such as encoding the data).

5.4 Anonymized and Aggregated Data

Anonymization is a data processing technique that disqualifies data from being personal data since once anonymized the data can no longer be associated with a specific individual. Examples of anonymized data include:

- Transaction data
- Click-stream data
- Performance metrics
- Fraud indicators (although personal data is used for this purpose, too)

We also aggregate data, combining large amounts of information together so that it no longer identifies or references an individual. We use anonymized or aggregate data for our business purposes, such as understanding user needs and behaviors, improving our Services, conducting business intelligence and marketing, detecting security threats, and training our algorithms.

The legal basis for processing the above mentioned data is the legitimate interest of a functioning app or website, business insights and fraud prevention.

6. How We Use the Data We Collect

6.1 General description

We must have a valid reason (or “lawful basis for processing”) to use your personal information. In some cases, the use of your personal information does not require your prior consent. We use your data for the following purposes:

- To provide and maintain our products and services under the User Terms. These services include:
    - The App where users can manage their World ID and digital tokens as well as learn about cryptocurrency in general and the Worldcoin project in specific;
    - The Operator App where Orb Operators can manage and oversee their Orbs under management and their statistics;
    - The P2P Marketplace where we connect users with agents (does not apply to users who are established or resident in Germany or have their habitual residence or registered office in Germany);
- To improve and develop our products and services, including to debug and repair errors in our Services.

- To conduct data science research.
- To analyze your use of our Services to provide better support.
- To enable you to publish information on a blockchain to prove your uniqueness.
- To use your wallet address to send you digital tokens we support.
- To comply with applicable law such as anti-money-laundering law and sanctions. This entails:
    - Using your IP address to block individuals whose country does not allow them to access the Services;
    - To answer data subject requests under the applicable data protection laws like requests for access or deletion;
    - Monitor potentially illicit financial flows e.g. from blacklisted wallets; and
- To comply with applicable law such as regulations against illegal content.
- To handle your customer service requests, complaints and inquiries.
- To resolve disputes, troubleshooting issues, and enforcing our agreements with you, including this Privacy Notice and the User Terms.
- To contact you regarding updates to the Services.

6.2 Credentials

TFH allows you to store certain credentials locally on your device to share them in the zero knowledge infrastructure of the World ID protocol ("Credentials"). In the context of Credentials we process this data in the following ways:

- We check the validity of your credential (in the case of passports this works through your country's root certificate).
- We authenticate you as the rightful holder of the credential (for passports this works locally on your device though a photo of your face (selfie) that is never stored).
- We encrypt, sign and store your credential's data in a secure environment on your device.
    - We never have access to the personal information contained on your credential.
    - You can then later selectively share this information with relying parties through the protections of the World ID protocol (e.g. you can prove that you are at least 18 years old without revealing your exact age or who you are).
- For passports, TFH only maintains an anonymized shard of a hash value of a unique cryptographic signature of your passport to ensure that each passport can only be verified once.

This processing is based on your consent and we never get access to your personal data from your passport which is stored on your device. You can delete this data from your phone by deleting the World App.

6.3 World ID Data

Your World ID (i.e. the secret number required to use it) is stored on your device only (in case you have a backup there exists an encrypted copy in your backup). Neither TFH nor anyone else have access to your World ID. You can use your World ID anonymously. Each time you use World ID with a new application, the application only receives a disposable number ("Nullifier") that does not reveal your World ID. This is enabled through Zero Knowledge Proofs (you only prove that you have a verified World ID but not which one) and ensures that your World ID cannot be used to trace you across applications. This means that World ID is not a general user ID for the internet.

World ID proofs function through an open protocol accessing a public Merkle Tree of the hashes of verified World IDs. World ID is not a centralized service but a protocol anyone can access. We offer APIs to facilitate access to the Merkle Tree and World ID Proofs but never receive any personal data in this context.

It is important to note that we also do not process any data related to your World ID that would allow us to identify you. All personal data processed in the context of World App particularly your wallet address and transaction data is deliberately designed to be delinked from World ID data.

7. Where We Process Your Data

7.1 Data Transfer.

When you provide us with your data, it may be transferred, stored, or processed in a location outside of where your data was originally collected. 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 make the best efforts to adhere to the principles stated in each jurisdiction regarding privacy laws. We only share data with data processors outside of your jurisdiction 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.

7.2 Risks of Transfer

Below is a list of possible risks that may arise if we transfer your data to the United States, the European Union, or another country. 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 at a GDPR level and fulfill 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.

7.3 Data Privacy Framework for US data transfers

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. TFH has 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. DPF. TFH has 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 Data Privacy Framework Notice 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 https://www.dataprivacyframework.gov/.

TFH is responsible for the processing of personal data it receives under the DPF and subsequently transfers to a third party acting as an agent on its behalf. TFH complies with the DPF Principles for all onward transfers of personal data from the EU, UK, and Switzerland, including the onward transfer liability provisions.

The Federal Trade Commission has jurisdiction over TFH's compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. In certain situations, TFH may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, TFH commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU and UK and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF should first contact TFH at dpo@worldcoin.org

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, TFH commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs)} and the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA) and the Swiss Federal Data Protection and Information Commissioner (FDPIC)} with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

For complaints regarding DPF compliance not resolved by any of the other DPF mechanisms, you have the possibility, under certain conditions, to invoke binding arbitration. Further information can be found on the official DPF website.

8. When We Share Your Data

We will never sell your data.

When we share your data outside of our organization, we will always:

- Share it in a reasonably 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.

We do share your data in these limited ways:

- **With Worldcoin Foundation:** we may act as Worldcoin Foundation processors for collecting personal data on behalf of Worldcoin (please check Worldcoin's privacy notice for further information).
- **Within our organization:** 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 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.

9. How Your Data is Recorded on Public Blockchain

Transaction information related to your use of our Services may be recorded on a public blockchain.

Please note: Blockchains are public ledgers of transactions that are maintained on decentralized networks operated by third parties that are not controlled or operated by Worldcoin. Due to the public and immutable nature of blockchain ledgers, we cannot guarantee the ability to amend, erase, or control the disclosure of data that is uploaded and stored on a blockchain

10. How We Use Cookies

We use cookies to help our Services work better. In addition to cookies, we may use other similar technologies, like web beacons, to track users of our Services. Web beacons (also known as "clear gifs") are tiny graphics with a unique identifier, similar in function to cookies. Our Cookie Policy, incorporated herein by reference.

We also use Google Analytics. More information on how Google uses your data when you use its partners' websites and applications: https://policies.google.com/technologies/partner-sites. By using the Services, you consent to us storing and accessing cookies and other data on your computer or mobile device and the use of Google Analytics in connection with such activities. Please read the information at the link provided so you understand what you are consenting to.

11. How Long Do We Keep Your Data?

Unless applicable law stipulates otherwise, we retain your data for as long as is reasonably necessary to provide our Services to you,

serve our legitimate business purposes, and comply with our legal and regulatory obligations. If you close your account with us, we will delete your account data within one month; otherwise we will delete your account data after 2 years of inactivity. If required by law, we will continue to 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.

Please note: Blockchains are decentralized third-party networks that we do not control or operate. Due to the public and immutable nature of blockchain technology, we cannot amend, erase, or control the disclosure of data that is stored on blockchains.

12. How this Privacy Notice Differs for Children and Teens

Individuals under the age of 18 are not allowed to use the Services, and we do not knowingly collect data from individuals under the age of 18. If you believe that your child under the age of 18 has gained access to the Services without your permission, please request the deletion of their data by contacting us through our Request Portal.

If we learn that we have collected data about a child under age 18, we will delete such data as quickly as possible. We have taken steps like implementing an automated age detection AI-model, instructions to operators and self-confirmations to restrict use of the Services to those who are at least 18 years old. We do not market products or services to children.

13. How to Contact us About this Privacy Notice

You may choose to delete your data from within the App under the Settings menu. If you have questions or concerns regarding this Privacy Notice, wish to exercise your rights, or to contact our Data Protection Officer (DPO), please submit your request through our Request Portal or write to us at Tools For Humanity Corporation, 548 Market Street, PMB 49951, San Francisco, CA 94104 USA or dpo@toolsforhumanity.com. We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws. You can also delete your data from within the World App.

If you have an unresolved privacy or data use concern that we have not satisfactorily addressed, please contact the data protection regulator in your jurisdiction. If you reside in the EU, then you can find your data protection regulator here.

If you reside in Thailand, you may contact our local representative in Thailand, Tilleke & Gibbins Digital Solutions Co., Ltd., at No. 1011 Supalai Grand Tower, 20th-26th Floors, Rama 3 Road, Chongnonsi, Yannawa, Bangkok, 10120 Thailand or email at digital@tilleke.com.

14. Your Rights

These rights apply insofar as we can identify the requestor in our database and insofar as we do not violate other data subject's rights by exercising the requestor's rights:

- 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 receive from us the personal data 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, provided the requirements for deletion under the applicable laws are given (e.g. several jurisdiction's laws oblige us to retain transaction information for a certain time period)
- You have the right to freely withdraw your consent to any data processing based on consent or to object to the data processing if it is not based on consent.

15. ADDENDA

In the following, several addenda provide legally required information for the respective markets we operate in. This information forms part of the consent depending on the region the data subject resides in. This information might differ from your location's information because we block certain services in certain jurisdictions. In case of any inconsistency with the above the more special statement about the particular jurisdiction prevails:

Addendum A: European Economic Area (“EEA”) and the United Kingdom (“UK”)

If you are in the EEA or the UK the following applies to you: You have at least the following rights You may have additional rights under General Data Protection Regulation, EU Regulation 2016/679 of 27.04.2016 (“GDPR”) as listed below. To exercise your rights available under GDPR, please contact us at our Request Portal. Apart from exceptional cases, we will resolve your request within the statutory deadline of one month. The use of the word GDPR in the following section also entails the UK-GDPR transposed into UK national law as the UK Data Protection Act of 2018 and retained as part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

A.1 The statutory rights under GDPR

This section applies if the processing of your data falls under the GDPR’s scope of application (*e.g.*, if you are a resident of the EEA or in the UK). You may have additional rights under GDPR as listed below. To exercise your rights available under GDPR, please contact us at our Request Portal.

- 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.

A.2 Data transfers

- When transferring data to a country that does not have an adequacy decision, we utilize the EU Standard Contractual Clauses. We are currently only transferring personal data to the USA.
- 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. Please also note that processing that is not based on consent is not affected by withdrawing the consent.

ADDENDUM B: JAPAN

If you reside in Japan, additionally, the following applies to you.

B1. Information Regarding the Japanese Regulations

We comply with Japanese laws and regulations, including the Act on the Protection of Personal Information of Japan ("APPI"). This section applies to our handling of "personal information" as defined in the APPI in precedence to the other portions of this Biometric Data Consent Form

We comply with Japanese laws and regulations, including the Act on the Protection of Personal Information of Japan ("APPI"). This section applies to our handling of "personal information" as defined in the APPI in precedence to the other portions of this Privacy Notice.

B2. Data Sharing

Unless otherwise permitted by applicable laws, we do not disclose, sell, provide, share, or transfer your personal information to any third party.

B3. Security Control Measures

We take necessary and appropriate measures to prevent any leakage or loss of, or damage to, your personal information being handled, and to otherwise maintain the security of personal information, such as by establishing rules for the handling of personal information, regular monitoring of the handling of personal information, regular training of employees in the handling of personal information, prevention of theft or loss of equipment used to handle personal information, and implementation of access controls. We also appropriately supervise our contractors and employees who handle personal information. You can obtain further details about the security control measures in place in relation to the handling of your personal information by contacting us at our Request Portal.

B4. Reference Information on Processing Personal Data in Foreign Countries

Your personal data is processed in the EU and USA.

B5. The Statutory Rights under APPI

To exercise your rights provided under the APPI please contact us at our Request Portal.

ADDENDUM C: ARGENTINA

If you are domiciled in the Argentine Republic, we inform you that the AGENCY OF ACCESS TO PUBLIC INFORMATION, in its capacity as Control Agency of Law No. 25,326, has the power to hear complaints and claims filed by those whose rights are affected by non-compliance with the rules in force regarding personal data protection.

The Agency can be contacted as follows:

Address: Av. Pte. Gral. Julio A. Roca 710, 5th floor - Autonomous City of Buenos Aires

Postal Code: C1067ABP

Phone number: (54-11) 3988-3968

E-mail: datospersonales@aaip.gob.ar

ADDENDUM D: SINGAPORE

If you are a resident of Singapore the following applies to you:

D1. Collection, use and disclosure of your personal data

If you are a resident of Singapore and with your consent, we will collect, use or otherwise disclose your personal data for each of the purposes as set out in our privacy notice. You may exercise your right to withdraw your consent at any time, but please note that we may not be able to continue providing our services to you depending on the nature and scope of your request. Please also note that withdrawing consent does not affect our right to continue to collect, use and disclose personal data where such collection, use and disclose without consent is permitted or required under applicable laws.[1]

D2. Exercise of your data subject rights

You may control the personal data that we have collected and exercise any of the rights by contacting us at our Request Portal. We aim to respond to your request as soon as we can, typically within 30 days. We will inform you in advance if we are not able to respond to your request within 30 days, or if we are not able to fulfill your request and the reasons.[2]

Where permitted by law, we may charge you an administrative fee to fulfill your request.

D3. Transfer of your personal data to other countries

If you are a resident of Singapore and we have collected your data, we may also transfer your data outside of Singapore from time to time. However, we will always ensure your personal data continues to receive a standard of protection that is at least comparable to that provided under the Singapore Personal Data Protection Act 2012, such as through the use of ASEAN Model Contractual Clauses.

ADDENDUM E – SOUTH KOREA

This Addendum for Korean Data Subjects explains our practices with respect to personal information we process in connection with your relationship with us where you are a Korean data subject.

E.1 – Transfer of Personal Information

We provide personal information to or outsource the processing thereof to third parties as specified below:

- Provision of Personal Information to Third Parties

Name of Recipient	Purposes of use by recipient	Items of personal information provided to the recipient	Periods of retention by the recipient
Tools for Humanity GmbH	The purposes described in this notice in section 6 above.	The items described in this notice in section 5 above	The storage periods defined in this notice in section 11 above.

- Outsourcing of the Processing of Personal Information to Third Parties:

Please find a list of all outsourced data processing and the respective companies under this link: https://www.toolsforhumanity.com/processors

We may outsource the processing of your personal information and/or transfer your personal information for storing purposes to third parties located outside of Korea:

If you do not want to transfer your personal information overseas, you can refuse by not agreeing to the transfer of personal information, or by requesting us to stop the cross-border transfer, but if you refuse, you may not be able to use our services. The legal basis for the cross-border transfer of personal information above is the fact that it constitutes "outsourced processing or storage of personal information that is necessary for the conclusion and fulfillment of a contract with the data subject" and statutorily-prescribed matters have been disclosed in the privacy policy (Article 28-8(1)(iii) of the Personal Information Protection Act).

E.2 – Destruction of Personal Information

When personal information becomes unnecessary due to the expiration of the retention period or the achievement of the purpose of processing, etc., the personal information shall be destroyed without delay. The process and method for destruction are set forth below:

1) Destruction Process: We select certain items of personal information to be destroyed, and destroys them with the approval of the DPO.

2) Destruction Method: We destroy personal information recorded and stored in the form of electronic files by using a technical method (e.g., low level format) to ensure that the records may not be reproduced, while personal information recorded and stored in the form of paper documents would be shredded or incinerated.

E.3 – Storage of Personal Information

If we are required to retain your personal information in accordance with applicable laws, we will do so for the following purposes and periods as required by applicable laws.

E.4 – Your Rights

You may exercise your rights related to personal information against us, including a request for access to, modification or deletion of, or suspension of processing of, your personal information as provided by applicable law including the Personal Information Protection Act. You may also exercise your right of withdrawal of consent to collection/use/provision of personal information, right to portability, and rights relating to automated decision-making. Such rights may also be exercised through your legal representatives or other duly authorized persons.

You may exercise any applicable rights described above by contacting us at worldcoin.org/requestportal.

E.5 – Security Measures

We will implement technical, organizational, and physical security measures prescribed by applicable Korean laws in order to protect personal information, such as those listed below:

1) Managerial measures: Designation of a Data Protection Officer, establishment and implementation of an internal management plan, regular training of employees on data protection, etc.;

2) Technical measures: Management of access authority to the personal information processing system, installation of an access control system, installation of security programs, etc.; and

3) Physical measures: Restriction of access to personal information storage facilities and equipment such as computer rooms and data storage rooms, etc.

E.6 – Contact Us

For questions or inquiries related to privacy and data protection, please contact our Data Protection Team at dpo@worldcoin.org.

ADDENDUM F – USA

The California Consumer Privacy Act, as amended by the California Privacy Rights Act, does not presently apply to us.

ADDENDUM G - BRAZIL

G.1 Applicable legislation, Controller and Operator

If you reside in Brazil, if your personal data was collected in Brazil, or if you use our Services in Brazil, the applicable legislation is the Law No. 13,709/2018 (General Data Protection Law, or "LGPD").

G.2 Right to object

You have the right to object to the use of your personal data for purposes that do not depend on consent if the purpose is inconsistent with the LGPD. If your objection is upheld, we will no longer use your personal information to develop and improve the features and experiences of our Services.

Note that if you do not provide or do not allow the collection or processing of certain personal data, it may affect the quality of your experience, we may not be able to fulfill the objectives of our Services, or we may not be able to provide certain Services to you.

In some cases, your data is anonymized, meaning it no longer identifies you. You cannot object to the use of anonymized data because it does not allow for your identification, as provided for in the LGPD. We use this anonymized data to improve our products and services.

G.3 The statutory rights under LGPD

According to the LGPD, you have the right to confirm the existence of processing, access, rectification, or request the portability of data processed. Moreover, you can request information of public and private entities with which we jointly use your personal data. You can also request information regarding the possibility of not giving consent and the negative consequences, and request the deletion of data processed with consent. You can choose the deletion of your information in the World App in the Settings menu.

Under certain circumstances, you have the right to object to or restrict how we process your personal data, or to withdraw your consent, which we rely on to process the information you provide.

You can exercise your rights under the LGPD by submitting a request to our DPO using the contact details in section H.4 below or through our online request portal. If you feel that your rights have not been adequately addressed, you can file a complaint with the Autoridade Nacional de Proteção de Dados Pessoais (ANPD) by completing the form available at this link: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados.

G.4 International Transfer of Your Personal Data

If the LGPD applies to you, and we have collected your personal data, we may also transfer it outside of the country. However, we will always ensure that your personal data is only transferred to foreign countries or international organizations that provide a level of protection adequate to that provided for in the LGPD, as recognized in adequacy decisions issued by the ANPD. In the absence of an adequacy decision, we will continue to follow a standard of protection that is at least equivalent to that provided for in the LGPD using Standard Contractual Clauses established in the ANPD's regulations or when we obtain your specific and highlighted consent for the international transfer.

ANNEX I – Legal grounds/purposes for Tools for Humanity data processing activities

Users

Why we Process the Data	**What Personal Data is Processed**	**Legal Ground for the Processing**	**Retention Period**
To create your account in World App	Wallet address, metadata, username	Performance of contract	Duration of the use of the services or until you request the deletion of the data.
To ensure you are of eligible age	Date of birth	Legal obligation	Your exact date of birth is never stored. We only store whether you are 18. We store this information for the duration of the use of the services or until you request the deletion of the data.
To optionally allow your contacts to easily communicate and transact with you	Phone number	Consent	Duration of the use of the services or until you request the deletion of the data.
To enable you to easily communicate and transact with your contacts	Address book contacts	Consent	Duration of the use of the services or until you request the deletion of the data.
To optionally show you Orbs near you	Location information	Consent	Up to 24 months.
To prevent fraud in the context of account prevention	Metadata, IP address, Device ID	Legitimate interest, namely the interest to prevent certain types of fraud (LIST OF TYPES)	Up to 24 months.
To ensure the service is permitted in your country	IP address, location information	Legal obligation	Up to 24 months.
To display your self-custodial wallet and provide an	Wallet address, transaction data	Performance of contract	No personal data is stored in this context.

interface for wallet transactions			
To display your self-custodial World ID and provide an interface for verifications	World ID information	Performance of contract	No personal data is stored in this context.
To display your self-custodial Credentials and provide an interface for sharing the Credentials	Credential information, credential validity information	Performance of contract	No personal data is stored in this context.
To analyze and improve our services and to conduct data science research	Usage data and metadata, public transaction data	Consent	Up to 24 months.
To comply with applicable laws such as anti-money laundering law, and sanctions	Transaction data, wallet address	Legal obligation	Duration of the use of the services.
To comply with applicable laws such as content regulations	Miniapp Content	Legal obligation	Duration of the use of the services.
To enable communication and marketing	Email address, push notifications	Legitimate interest	Up to 24 months.
	Correspondence from you	Legitimate interest	Up to 24 months.
	Feedback from you	Legitimate interest	Up to 24 months.
To handle your customer service requests, complaints and inquiries.	Communication information and email or social media profile name if you seek to communicate with us through such means	Performance of contract	
To make sure the app is running smoothly for you	Metadata	Performance of contract	Up to 24 months.
To verify your device	Device World ID data (device fingerprint)	Performance of contract	Duration of the use of the services.
To resolve disputes, troubleshooting issues, and enforcing our agreements with you, including this Privacy Notice and the User			Duration of the use of the services.

Terms.			

Business partners

Why we Process the Data	**What Personal Data is Processed**	**Legal Ground for the Processing**	**Retention Period**
Communication	Phone number, email address, Name	Legitimate interests, i.e. the interest to communicate with business partners.	Duration of the business relationship or until you request the deletion of the data.
Maintaining and administering a business relationship	Phone number, email address, Name, enterprise data	Legitimate interests i.e. the interest to maintaining and administering a business relationship with business partners.	Duration of the business relationship or until you request the deletion of the data.
Fulfill KYC obligations	Passport data, Enterprise data	Legal obligation	Duration of the business relationship and up to 3 years after termination.
To process your application	Application data	Consent and steps at the request of the data subject prior to entering into a contract.	Up to 3 months by default or longer if you agree to be part of a talent pool.