Title: Understanding Personal Custody and its benefits
URL: worldcoin.org/blog/worldcoin/understanding-personal-custody
Meta:

User-centric architecture is an important part of the Worldcoin Tech Tree. It gives you control of your data in a way that you don't have with other online experiences.

When you, the user, take center stage, it's easier to separate and replace other system components like "orbs" and "uniqueness"—separation that's necessary to build an open, permissionless protocol that can be owned and governed by the largest number of people possible (learn more about this here).

That's why Worldcoin is implementing Personal Custody, first announced with the introduction of World ID 2.0. With Personal Custody, optional Data Custody will no longer be offered at the time of your orb visit. This helps ensure everyone can learn about Worldcoin before deciding whether or not to share their information to help improve the project.

What is Personal Custody, and how does it benefit you?

Personal data custody, or Personal Custody, means that the information (images, metadata and derived data) generated at the orb and used to generate the iris code during World ID verification is held on your device. **This approach gives you control over the flow of this data**—not just deletion, but any future use prior to being deleted. Previously, this information was deleted by default.

In addition to giving you control, Personal Custody unlocks new World ID use cases by enabling Face Authentication for high security applications. With Face Authentication, you can verify at any time that you are the same person that received your World ID when verifying at an orb. Importantly, this works **locally on your device, without your data leaving your phone**.

For Worldcoin, giving you control over your data flow with Personal Custody is a significant step towards solidifying the project's user-centric architecture and building an even more robust and secure World ID network.

How does Personal Custody work?

At a high level, Personal Custody involves four components: your device, the orb, a data package containing your images and a temporary backend storage for transit. Importantly, *the backend cannot decrypt your data package*.

Here's how the process works:

1. Your phone generates a public-private key pair to encrypt your data, then transfers the public key to the backend.
2. The backend generates additional keys for all data that requires double encryption and passes the public keys to the orb.
3. During verification, the orb creates the necessary images to verify your World ID.
4. The orb then creates your individual data packages, encrypts them, “signs” them to ensure authenticity and security, then sends them to the backend before deleting the images.
5. Your encrypted data packages are downloaded to your phone prior to their deletion from the backend.

Since all data is encrypted by your public key, the end result of this process is a collection of encrypted data packages that reside exclusively on your device. The use of double encryption within the end-to-end encryption envelope is a safeguard to protect the confidentiality and privacy of your data in the event your phone is compromised.

The illustration above is designed to help visualize the flow of keys and data throughout this process. The files cannot be decrypted by either Worldcoin or Tools for Humanity, and the system has been designed to intentionally keep your data secure even in the case of a potentially malicious actor.

Learn more

For more information on the orb, privacy and the Worldcoin Tech Tree, see the Technical Implementation section of the Worldcoin protocol whitepaper.

You can also learn more about the Worldcoin protocol by visiting the Worldcoin website, joining the daily conversations on Twitter/X, Telegram, Discord, YouTube and LinkedIn, or signing up for the blog newsletter at the bottom of this page.