

## DATASHEET

# User Privacy

Protect user data with a privacy-by-design identity verification and authentication framework



Managing user data poses significant risks for organizations. Without proper safeguards, sensitive personal information becomes vulnerable to theft and misuse, undermining trust between users and service providers. Protecting user privacy isn't just a legal requirement; it's a moral imperative and, when done right, can be a competitive advantage.

### **The 1Kosmos BlockID Privacy by Design**

By design, 1Kosmos offers a comprehensive solution to address the challenges of effectively managing user privacy. Leveraging advanced technologies like blockchain and biometrics, 1Kosmos provides secure identity verification and authentication, ensuring that users' personal information remains protected against unauthorized access and misuse.

The privacy and security of user biometrics and other personally identifiable information (PII) comply with GDPR and 230 other GDPR-like regulations worldwide.

This privacy-by-design approach enables end users to view and approve or reject the sharing of all information requested by online services they wish to access. All personally identifiable information (PII) is encrypted end-to-end and never exposed.

Users approve or reject sharing requests directly with the applications to which they connect without any third-party intermediary having access to their data - no external public key server, host messaging server, etc., have access to the keys or plaintext messages.

Additionally, 1Kosmos and its customers cannot access the user data.

The captured PII data is encrypted and written to our private and permissioned blockchain, ensuring privacy, security, and complete auditability. Only the enrolled user can access the private key required to access and share their information at any time and with any online service.

**The 1Kosmos privacy by-design framework solution exceeds FIDO, NIST 800-63-3, UK DIATF, and iBeta DEA EPCS security standards.**



## 1KOSMOS FEATURES AND BENEFITS

- Privacy Preserving – Unilaterally increase privacy and security, an industry first.
- Privacy by Design – PII data is not accessible by 1Kosmos or our customers.
- Consent – Users are in control of how and when data is shared. Cannot be shared without consent.
- Secure Biometrics – Deployment of biometrics are GDPR, BIPA, CCPA, etc. exempt.
- Phishing Resistant – Protect employees and security teams from making a mistake.
- Advance Privacy-Preserving Data Sharing and Analytics (PPDSA) - aligns with the new US National Strategy.

### Reasons to Consider

- Certified solution to FIDO2, UK DIATF, iBeta DEA EPCS, and NIST 800-63-3
- Compliant with GDPR and KYC / AML

## About 1Kosmos

©2024 1Kosmos Inc., All rights reserved. 1Kosmos BlockID is a distributed digital identity platform supporting both business-to-employee and business-to-consumer services that easily integrates with existing operating systems, applications, and IT security infrastructure to perform strong, verified identity-based authentication – eliminating the need for passwords, one-time codes, and more. By simplifying identity infrastructure, 1Kosmos drives both cost savings and user convenience while securing businesses and individuals from the harm and inconvenience of identity fraud.

## Certification and Compliance

1Kosmos BlockID is certified to FIDO2, NIST 800-63-3, iBeta DEA EPCS, UK DIATF, SOC2 and ISO 27001. Our platform ensures there is no central honeypot of user information or a user store for hackers to attack. 3rd parties do not have administrative access to user information.

## User Managed

1Kosmos empowers users to have the authority to govern the sharing and exposure of their data. Users are given a private key at the time of onboarding, to control access to personally identifiable information (PII). This means that only the user, with their unique private key, can access their PII data, guaranteeing utmost security and privacy.

## Consent

Immediately after an end user downloads the 1Kosmos BlockID app, the application requires the end user to acknowledge the general consent conditions, including the validation of the end user's documents. After consent, captured data will be under the user's control. The PII data can now only be shared with the user's explicit consent to do so.

## Data Capture

The capture and storage of end-user data will be managed on the end-user device (phone) or web wallet (if appless). The end user will fully control saving, sharing, and deleting the information. The end user will continue to have full control when data is shared with service providers. 1Kosmos offers customizable data retention policies. By default, no identity data is retained, ensuring maximum privacy and security.

## Advance Privacy-Preserving Data Sharing and Analytics (PPDSA)

1Kosmos includes the use of privacy preserving technologies, including on-device processing, neural network cryptography, and fully homomorphic encryption (FHE) to protect each user's biometric privacy and exempt the system from privacy law obligations.