Feedback for “Guidelines 02/2025 on processing of personal data through blockchain technologies”

by ARPA CORP. and ARPA Hellenic Logical Systems
Author: Ross Peili (r1@arpacorp.net)

On-Chain Personal Data & Access Control:

- The primary concern isn't storing personal data on-chain *per se*, but controlling *access* to it. Blockchains serve as immutable records of activity, and personal data within them can be valuable for user protection, verification, and evidence.
- The focus should shift towards robust access control mechanisms ensuring only the data subject (and potentially autonomous systems acting strictly in the user's interest or per predefined rules) can access sensitive data. Data stored on-chain, if properly secured, shouldn't inherently pose a threat if human/organizational access is strictly governed.

Defining Personal Data & De-anonymization Realities:

- Given the existing infrastructure (cloud, hardware) and the history of encryption standards (like SHA-256 originating from state agencies), it's prudent to assume that powerful state actors or sophisticated entities *could* potentially de-anonymize wallets or even compromise data, despite cryptographic protections. Historical events like the Ethereum fork demonstrate that human intervention can override supposed immutability when deemed necessary.
- Therefore, reliance solely on current cryptographic techniques for anonymization might offer a false sense of security. Advanced, user-controlled access mechanisms are paramount.

Biometric & User-Centric Access Control:

- To truly secure on-chain personal data, consider incorporating biometric verification (e.g., non-transferable DNA markers tied to wallets via NFTs, liveness proofs) as a fundamental access layer. This ensures only the legitimate owner can access or grant permissions to their data, even if traditional credentials (keys, passwords) are compromised.
- Access requests (e.g., from institutions like hospitals or law enforcement) should be granular, time-bound, purpose-limited, and require explicit, verifiable consent from

the data subject via these secure mechanisms (e.g., through purpose-specific smart contracts). Data minimization principles should apply strictly to any granted access.

Smart Contracts for Data Governance & Legacy:

- Smart contracts offer powerful tools for automated data governance based on user pre-definitions. Examples include self-executing last wills for digital assets and data, triggered by verified events (e.g., signals from health tech providers), bypassing traditional intermediaries.
- Biometric verification can also serve as a master recovery mechanism for private keys, enhancing user control and security beyond traditional methods.

Security & Quantum Computing Context:

- While acknowledging future threats like quantum computing is important, the immediate focus on it relative to blockchain security may be disproportionate. Quantum capabilities would likely pose systemic risks across *all* critical digital infrastructure (banking, power grids, communications) long before targeting specific blockchains becomes the primary concern.
- Furthermore, the development of quantum computing is currently centralized and observable, and quantum cybersecurity measures will likely evolve concurrently. Overstating the near-term, specific risk to blockchains from quantum actors, while potentially understating existing vulnerabilities or state capabilities, could skew priorities.