Comments on EDPB Guidelines 02 2026 on Anonymisation

29 October 2026

Submitted by Hervé Lacorne in a personal capacity, drawing on his work as CEO of World KYC, a Winstant brand and product, and co-founder of Trade Enabler.

Purpose of this response

I submit these comments in a personal capacity, drawing on my work with World KYC. I request practical guidance on selective proofs, relationship-specific identifiers and accountable identity custody. Businesses should be able to establish a necessary fact without routinely collecting the documents and attributes behind it. Individuals should be able to participate under different identities in different contexts, while legitimate accountability remains possible through properly governed custodians. This approach seeks to make unnecessary identification more difficult while preserving controlled communication and lawful accountability.

I welcome the contextual approach in Guidelines 02/2026. The distinction between the recipient's situation and the custodian's situation is particularly relevant to my work. I also recognise that this distinction cannot be used to disregard processing roles, identifying information available elsewhere, or routes through which identification can occur. Guidelines, paragraphs 6–15.

My main request is for worked examples and an assessment template covering three situations: age assurance, research participation and financial eligibility. These should help organisations distinguish genuinely anonymous outputs from useful privacy-preserving processing that remains within data protection law. I seek clarification applicable to different technologies, not endorsement of World KYC or a special legal category for World KYC’s products.

Operational context

World KYC has a presence in Thailand and Belgium and is open to prospective notary-node partners. Discussions and partnership arrangements are at different stages in jurisdictions including France, the United States, Australia, Canada and Korea. The account below describes capabilities World KYC reports as available today, rather than results of an independent certification or anonymity assessment.

I am also co-author, with Tobias Endress, of the chapter Deposit Tokens, Stablecoins, and the Evolution of Digital Settlement in the forthcoming volume Digital Project Practice to Capitalize on Digital Assets and Virtual Currencies, edited by Tobias Endress (Auerbach Publications; publisher copyright 2027).

Trade Enabler — Enable Trade. Prevent Fraud. Preserve Privacy. — SWIFT Hackathon 2026 finalist.

Users can create one or several Stealth IDs and keep them active or revoke them. They may use a separate identifier for each relationship, but can also choose to reuse an identifier across businesses. Pairwise separation is therefore an available configuration, not a universal property of every deployment. A service may request an age bracket, another a particular eligibility result, and another additional attributes relevant to its purpose. Sharing is restricted to authenticated counterparties, with the individual choosing what to disclose, subject to applicable legal obligations.

Identity records are held through notary trustees under a distributed custody model rather than a single central identity repository. Administrative separation is intended to isolate information across nodes. Where reconciliation is necessary, World KYC's model uses authenticated shared counterparties. That reconciliation pathway must itself be included in any assessment; distribution does not make a possible identification chain disappear. I use "notary" here to describe the trustee and custody function, without asking the EDPB to presume a particular legal status from that label.

Zero knowledge notarisation

I use zero-knowledge notarisation to describe an arrangement in which the notary verifies and retains underlying identity evidence while the recipient receives only the permitted attestation, without the supporting identity information. This describes the allocation of knowledge between parties; it is not a claim that every implementation uses a cryptographic zero-knowledge proof or that every resulting record is legally anonymous.

The analogy is to a traditional notary checking evidence and issuing an attestation, rather than passing the supporting file to every recipient. The recipient learns the selected fact needed for the interaction, while the notary remains responsible for the evidence in its custody.

Double Pendulum Privacy

World KYC's Digital Identity 2.0 white paper, sections 3.4–3.5 (World KYC, n.d.; accessed 29 October 2026), describes V-Links and a double-pendulum architecture based on contextual separation and structural isolation. The Double Pendulum Privacy Model on World KYC's website describes independent identity contexts for people, businesses and products.

In the relationship-specific configuration discussed here, separate aliases can reduce cross-context linkage, while segregation between custodians can limit the consequences of a compromise. Reused aliases, shared administrators, recovery routes and reconciliation mechanisms must nevertheless be evaluated as possible linkage paths. These objectives require examination of the actual configuration, information flows and controls. Attaching a V-Link to information cannot, by itself, establish that its contents are anonymous.

1 Assess the information and each relevant relationship

For paragraphs 6–15, 37 and 51, I propose a practical assessment record identifying the information being assessed, the intended recipient, the recipient's purpose, the custodian, any intermediaries and their respective roles. The record should distinguish the proof presented to a business from the supporting records retained elsewhere and from associated account, transaction or communication records.

World KYC provides the technology layer for automated connectivity and authenticated communication; the notary-node operator verifies and holds the identity records. Notary nodes apply a strict baseline of identity verification under their own applicable legal obligations, rather than simply following each relying business's instructions. An issuer may separately specify additional requirements for a V-Link or wallet, such as residency or accredited-investor status under the relevant rules, and which verification providers or notaries it accepts. The assessment should distinguish common identity verification from checking these issuer-specific conditions.

These functions require separate assessment of who determines the purposes and essential means; neither the node label nor an issuer's requirements automatically settles the controller or processor classification. The role of the technology provider must likewise be assessed separately from that of the node operator. Financial institutions retain their applicable local obligations. The approved-provider arrangement is conceptually comparable to the counterparty-permission controls of SWIFT's Relationship Management Application: a relying institution decides whose attestations it will accept and for which purposes. This is an analogy about permissions, not a claim of SWIFT integration, certification or equivalent legal effect.

The template should also identify the recipient's ability to recognise the same person again. A new alias for every relationship and a common alias used across several services are materially different designs. Reuse should be visible in the assessment rather than hidden behind a general description of the platform as decentralised or privacy-preserving.

Examples 3 and 4 accompanying paragraph 15 distinguish processing on behalf of a controller from independent use by a recipient. I ask the EDPB to extend that contrast to a custodian retaining the identity mapping while a recipient receives a limited proof, with or without a persistent alias. The example should state the facts needed to reach an outcome and the changes that would alter it. This would make the assessment usable without encouraging the assumption that a recipient's lack of direct access to identity documents settles its legal position.

Authenticate the receiving organisation

Before disclosing personal information, the receiving organisation should itself be authenticated, with its legal identity and jurisdiction made clear to the individual. An LEI can anchor that identification to verified entity reference data; where available, a verified vLEI role credential can help establish the identity and role of the person acting for it. The disclosure process must separately establish the requester's authority for the specific purpose, necessary attributes, lawful basis and secure channel. This reciprocal identification can reduce impersonation risk and improve cross-border accountability without requiring unnecessary disclosure by the individual.

2 Distinguish minimal proofs from persistent identities

I recommend additional examples alongside paragraphs 19–25, 50–51 and 98–103. The guidelines recognise identification through distinguishing a person, including without knowing their name, while also distinguishing record isolation from actual identifiability. Guidelines, paragraphs 19, 25 and 98–100.

A stable alias that enables a recipient to recognise, contact or treat the same person differently remains personal data for that recipient, even where civil identity is not disclosed. Relationship-specific aliases can reduce cross-context linkage without making those ongoing interactions anonymous. My request concerns identifying narrower outputs that may satisfy the contextual anonymity test, rather than a blanket exemption for persistent accounts.

The examples should address three separate questions: what attributes are disclosed, whether presentations can be linked, and whether the recipient can recognise or act upon the same individual. These questions arise in the following proposed cases.

Age assurance

A service needs to determine whether a visitor meets an applicable age threshold, such as 16 or 18 in a particular context. Instead of receiving a date of birth or identity document, it receives an authenticated result establishing that the required condition is satisfied. The example should not prescribe either threshold as a universal legal rule.

Building on the tokenised age-threshold approach in Statement 1/2025 on Age Assurance, paragraph 20, I ask how the anonymity assessment changes between a one-off result and a result attached to a persistent account or alias. The comparison should include network and device information, timestamps, verification logs and other information available to the recipient. It should explain whether and how these surrounding records affect the assessment of the proof.

This would help businesses understand when they have reduced disclosure but still process personal data. The example should also distinguish an eligibility result from an authentication status. Failure to establish a condition need not mean that the person fails the condition; evidence may be unavailable, expired or unsuitable.

Research participation

A person first establishes that they fall within a study's permitted age bracket, then participates using a project-specific alias. Researchers communicate through authenticated alias email, notes or chat without routinely receiving the participant's civil identity. The custodian retains the identity relationship required for an authorised disclosure or contact process.

I request separate assessments of initial screening, longitudinal participant records and a later dataset provided to an independent analyst. The ability to recognise the same participant and send individual follow-up messages should be considered explicitly. Health information, unusual characteristics and the circumstances of recruitment may also create identification opportunities independent of the alias.

This example should preserve the distinction between minimising identity disclosure during a study and establishing the anonymity of a particular research output. A finding that operational records remain personal should not obscure the practical protection offered by separating identity custody from routine research access.

Example 22, paragraph 94, illustrates contextual assessment after the original personal data have been deleted; the present example additionally asks how retained custody records and continuing participant contact affect each relevant perspective.

Financial eligibility

A service seeks evidence that an individual satisfies a defined financial eligibility condition. It receives the relevant result instead of the underlying identity documents and detailed financial records. The example should specify the applicable rule, jurisdiction, evidence standard and validity period, rather than using “eligible investor” as an undefined status.

An authenticated wallet provides a further example. An issuer may receive an attestation that its holder satisfies a specified eligibility requirement, without receiving the underlying identity documents or publishing those documents on-chain. The attestation should identify its scope, responsible custodian, validity and revocation conditions. Trade Enabler, which I co-founded, describes this application of World KYC as governance before settlement: checking the required authorisations and eligibility conditions before a transaction proceeds.

I ask the EDPB to distinguish the eligibility proof from the individual's account and transaction history and from retained compliance records. An anonymity assessment should not be represented as permission to disregard a separate identification, verification or recordkeeping duty. Equally, where the recipient does not need the underlying documents, the example should show how unnecessary duplication can be avoided.

Privacy from public blockchain observers must be distinguished from the identification and information-sharing obligations of regulated participants. Where the Travel Rule applies, the relevant regulated entities must obtain, retain and securely transmit the required originator and beneficiary information as applicable, and make it available to competent authorities under applicable law. FATF’s October 2021 guidance, paragraph 188, permits secure transmission outside the blockchain; Regulation (EU) 2023/1113, Article 14(4), likewise does not require the information to be attached to the crypto-asset transfer, while preserving its timing, security and data-protection requirements. A notary-mediated architecture may support this separation, but its compliance depends on the participating entities, information flows and jurisdiction-specific requirements.

3 Explain lawful disclosure and identification chains

MRLTBU, or “means reasonably likely to be used”, should be translated into a practical account of who can obtain what information, from whom and through which route. Paragraphs 20–21 and 28–34 address third-party identification chains, lawful access and the limits of contractual restrictions. Guidelines, paragraphs 20–21 and 28–34.

I request an example contrasting a recipient with a legally available identification route, a recipient effectively prevented from using such a route, and a competent authority able to obtain relevant information. The assessment should identify the powers and relationships actually applicable to each actor. It should neither assume that all recipients possess every authority's powers nor exclude a route merely because it is described as exceptional.

My proposed governance baseline for custodial disclosure includes verification of the requester and legal basis, review independent of the commercial requester, attention to the scope of the request, disclosure limited to the applicable requirement, an auditable decision record, and notice or an opportunity to challenge where legally permitted. These are proposed safeguards to document and evaluate, not claims that they automatically establish anonymity or override binding legal duties.

Ordinary disputes should also be distinguished from compelled identification. Authenticated alias communications may allow questions or complaints to be resolved without disclosing civil identity. The EDPB could illustrate how such mediated contact affects identifiability from the perspectives of the relay and the custodian.

An assessment should distinguish physical hosting location, technical control, legal responsibility for processing, and the legal powers that may compel disclosure. Relevant facts include where primary data and backups reside; who operates the infrastructure and administers the service; who controls decryption keys and recovery mechanisms; which parties can access plaintext; and which laws apply to those parties. In a hypothetical example, a Cambodian identity custodian might use Singapore hosting for resilience. Neither location alone determines the custodian’s responsibilities nor excludes the host’s technical or legal exposure. GDPR controller and processor roles must be assessed separately from the descriptive label “custodian”.

4 Test separation and the effects of revocation

For paragraphs 44–51 and 90–93, I propose a configuration-level checklist for architectures using several identifiers or custodians. It should record whether aliases are reused; where identity mappings, keys and recovery information exist; which administrators can access them; and how information could be combined through shared counterparties or other intermediaries. It should also distinguish hosting and backup regions, infrastructure operators and subprocessors, relevant legal entities, privileged support access, key custody, plaintext exposure during processing and the routes through which lawful disclosure could occur.

Testing should include ordinary operation and credible failure paths: compromised credentials, account recovery, administrator misuse, collusion, repeated presentations and information disclosed through status or revocation checks. Relevant controls should be evaluated for their effect on the actual identification route, rather than assumed effective because a system is described as distributed.

Testing should also establish whether a custodian or communication relay can observe relationships across services, and whether credential identifiers, signatures, status references or other recurring metadata permit linkage despite different aliases.

Revocation needs particular clarity. World KYC’s system supports revoking identities, but I do not equate revocation with erasing material already viewed, copied or lawfully retained by a recipient. I request an example distinguishing termination of future use from the continued existence and identifiability of historical records. It should also address whether changing an identifier actually breaks linkage when other connecting information remains.

Multiple profiles belonging to one person should be distinguished from unauthorised impersonation. Similarly, an authorised AI agent should be distinguishable from the human or organisation on whose authority it acts. For anonymity assessment, the relevant questions include what those attestations reveal, what persistent references they introduce and who can resolve the underlying relationship. I do not propose that an automated agent should be described as a verified human.

5 Make the assessment usable for smaller organisations

For paragraphs 35 and 37–42, I request a concise assessment template that smaller organisations can maintain and that providers can support with deployment-specific evidence. Custodian accountability and transparency remain important where originals are retained; documentation and reassessment should reflect the processing actually performed. Guidelines, paragraphs 35 and 37–42.

The record could identify the use case, actors, disclosed fields, retained records, identification routes, tests performed, unresolved assumptions and responsible reviewer. Reassessment triggers could include a change in identifier reuse, a new reconciliation function, a security incident, additional available datasets or changes to relevant legal access.

Providers should make configuration choices understandable. A business should know whether it is receiving a one-off proof, a stable alias or a reusable cross-service identifier, and what each choice means for retention and recognition. This would make privacy-preserving services more useful to SMEs without implying that using a provider removes their responsibilities.

Conclusion

I ask the EDPB to add the worked examples and practical assessment tools described above. They would help organisations reduce unnecessary identity collection while making defensible distinctions between anonymous outputs, pseudonymous interactions and identifying records retained for legitimate purposes.

My objective is accountable participation with less routine disclosure of identity. Clear guidance should support that objective while requiring evidence for every claim of anonymity, including claims made for V-Links, selective proofs and distributed custody systems.