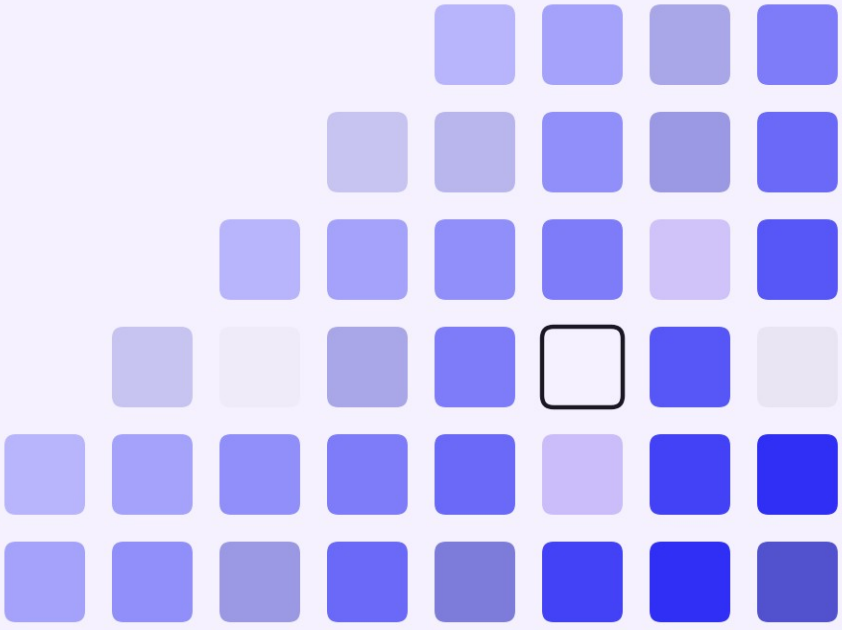
EUROPEAN ETHEREUM INSTITUTE

ethereum.institute

PUBLIC CONSULTATION

Response to the EDPB Guidelines 02/2026 on Anonymisation



Brussels, 30 October 2026

Response to the EDPB Guidelines 02/2026 on Anonymisation

The European Ethereum Institute
October 2026

What we ask the Board

> **First.** State in the final text of the anonymisation guidelines that a commitment computed under a perfectly hiding scheme, whose input data and witness have been deleted, is anonymous information within the meaning of Recital 26 GDPR, subject to the conditions set out in Section 4, and set out the state-of-the-art criteria the Board expects for such schemes.
>
> **Second.** Confirm that "rendered anonymous" in the blockchain guidelines is assessed under the anonymisation guidelines, and make clear which designs satisfy both texts, including where an institution must first keep its records for the full period that anti-money laundering law requires and can delete or anonymise them only once that period has ended.
>
> **Third.** Confirm that validators applying the protocol's uniform rules, without discretion over which transactions are included, are assessed from their own perspective and are not in a position to identify anyone in the sense of paragraph 19; explain how paragraph 21 applies to the publication and relay of data on a public ledger; and clarify that the closing sentence of paragraph 96 states a goal for anonymising controllers and does not displace a finding of anonymity from a particular entity's perspective.
>
> **Fourth.** Recognise that the hiding property of a perfectly hiding commitment does not weaken over time.

The European Ethereum Institute welcomes the Board's consultation on Guidelines 02/2026 on Anonymisation.[1] Our response concerns how they apply to data recorded on public blockchains, and in particular how they fit with Guidelines 02/2025 on processing of personal data through blockchain technologies, adopted in their final version at the same plenary. We refer to the two texts below as the anonymisation guidelines and the blockchain guidelines.

The blockchain guidelines repeatedly allow controllers to meet storage limitation, consent withdrawal and erasure by deleting data **or rendering it anonymous**, while the anonymisation guidelines set the test for whether data is anonymous. How the two texts fit together therefore decides which blockchain designs give controllers a workable route to compliance. **Our main proposal is that the final text recognise as anonymous a commitment computed under a perfectly hiding scheme once its input data and witness have been deleted, which is the result paragraph 53 of the blockchain**

[1] European Data Protection Board, Guidelines 02/2026 on Anonymisation, Version 1.0, adopted 7 July 2026 for public consultation; European Data Protection Board, Guidelines 02/2025 on processing of personal data through blockchain technologies, Version 2.0, adopted 7 July 2026.

guidelines already describes without qualifying it in law (Section 3). We also ask the Board to align the two texts on the standard for rendering data anonymous, and to confirm how actors that cannot identify anyone, such as nodes, are assessed (Sections 2, 8 and 9).

1. The gap between the two sets of guidelines

The blockchain guidelines treat the forms in which data may be recorded on a chain differently. Encrypted personal data and salted or keyed hashes remain personal data (paras 51 and 52), and paragraph 104 advises against recording either. Commitments are in a different position. Paragraph 53 states that where a commitment is computed with a perfectly hiding state-of-the-art scheme, once the original data and its witness are deleted, the commitment left on the chain is useless, and it is neither possible to recover nor to recognise the original data, and commitments are not among the forms paragraph 104 advises against. **Neither text says whether that residual commitment is still personal data.**

The gap matters because the blockchain guidelines rely on anonymisation as the alternative to deletion: once the purposes have been achieved (para 60), when consent is withdrawn (para 71 and Recommendation 9), at the end of the retention period (para 80 and Recommendation 11), and on an erasure request or objection (para 103 and Recommendation 16). Paragraph 103 describes the mechanism, the erasure of off-chain data that would allow indirect identification, and paragraph 64 the outcome, an anonymised transaction that still allows the integrity of the remaining transactions to be verified. None of these passages says which test decides whether what is left on the chain is in fact anonymous, and the anonymisation guidelines, which set that test, do not mention commitments.

2. Where responsibility lies on a public blockchain

The anonymisation guidelines assess identifiability from the perspective of each relevant entity, so that the same information can be anonymous for some entities and personal for others (paras 6 and 7), in line with *EDPS v SRB*.[2] On a public blockchain, the relevant entities hold very different information, and it helps to distinguish four layers, shown in Figure 1. The **application layer** is the organisation that decides what is written to the chain, for example, a university that wants its diplomas to be verifiable, and will normally be the controller for that processing (blockchain guidelines, para 38). **Off-chain storage** is that organisation's own systems, where the personal data itself should be kept (para 54 and Recommendation 2). The **base layer** is the ledger and the nodes that replicate it; nodes with only limited decision-making power might not be controllers, and in certain cases nodes on public permissionless chains do not act on behalf of any controller (paras 42 to 44).

[2] C-413/23 P *EDPS v SRB*, judgment of 4 September 2025.

The **access and ecosystem layer** covers the services through which people reach the chain, such as wallets, exchanges and block explorers (para 14). These services hold very different information, and wallets in particular come in two kinds. A **custodial wallet** is a service in which a provider keeps the keys, and so controls the assets, on its clients' behalf. That is custody and administration of crypto-assets under MiCA, and its provider, like an exchange, is a crypto-asset service provider that identifies its customers and must keep customer identification and transaction data for at least five years under MiCA and EU anti-money laundering rules, as the Board itself notes (footnote 43). Under the Transfer of Funds Regulation it must also obtain and hold information on its customers' transfers to and from self-hosted addresses and, above EUR 1,000, assess whether such an address is owned or controlled by its customer.[3] Its records can therefore link to a person not only the accounts its customers hold with it but also addresses that its customers control themselves.

A **self-custodial wallet** is software with which the user holds their own keys. Its provider does not hold the keys or the assets, does not identify the user, and is outside the scope of MiCA (Recital 83). Some providers screen the addresses a user is about to transact with against sanctions lists or commercial risk data, which does not require the provider to know who its user is. Operators of interfaces to decentralised applications do the same. What a self-custodial wallet provider may hold is operational data, such as the IP address of a device that connects to a server it runs, which the blockchain guidelines treat as personal data generated off the chain (para 28). For that processing, it is responsible like any other controller. For the ledger itself, it holds no more than a node does.

This matters because identifiability is assessed entity by entity. A node operator in the base layer usually holds nothing but the ledger, and as far as on-chain data is concerned, so does a self-custodial wallet provider, while an exchange or a custodial wallet provider may hold the additional information that turns an address into a direct connection to a person. These are also the entities on which the law already places the obligation to know who is behind an address.

[3] Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), Art 3(1)(16)(a) and (17), and Recital 83; Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, Arts 14(5) and 16(2).

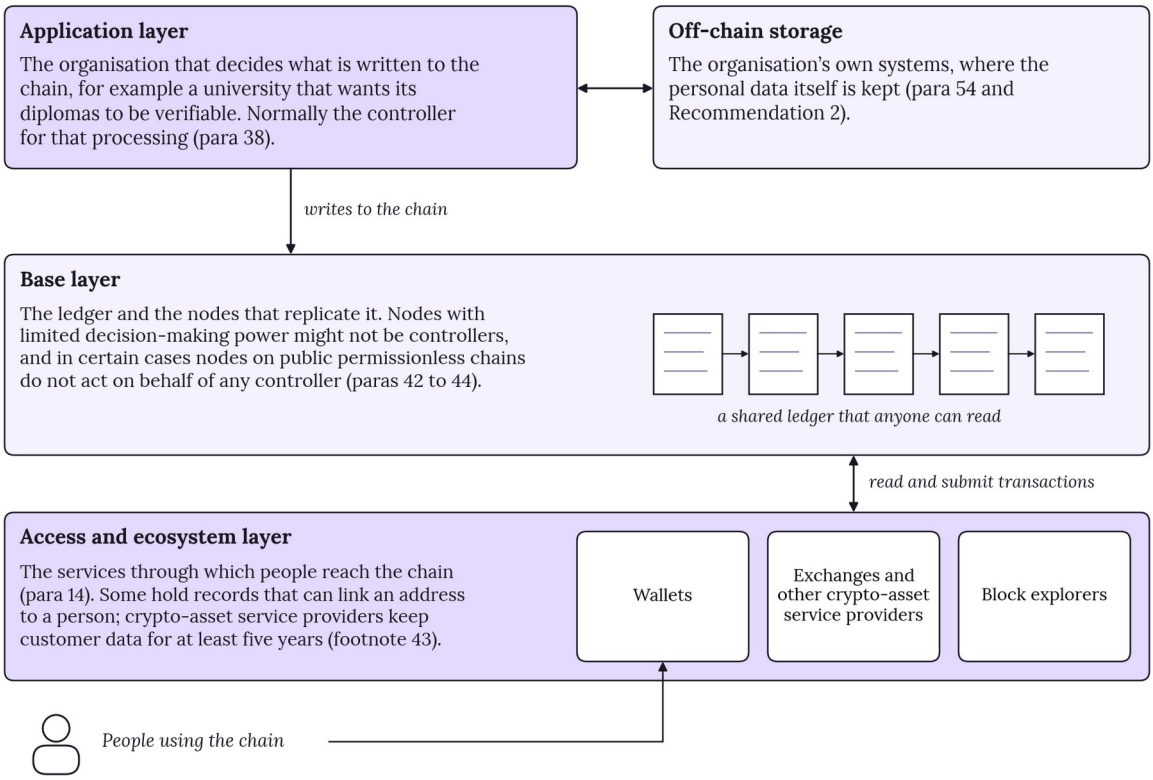


Figure 1. The four layers of a blockchain-based service, what each holds, and how the guidelines treat it.

Paragraph 19 defines identification as distinguishing a person from others in a given context so that they can be treated differently, and the second element recurs throughout the guidelines (para 16(c), para 87, and Examples 6 and 24). Being able to tell one record from another is therefore not sufficient. The question is whether the entity holding the record can, by means reasonably likely to be used, act differently towards the person to whom it relates, bearing in mind that additional information kept under appropriate security controls counts as accessible only to authorised users (para 89). Figure 2 applies this to a single Ethereum transaction.

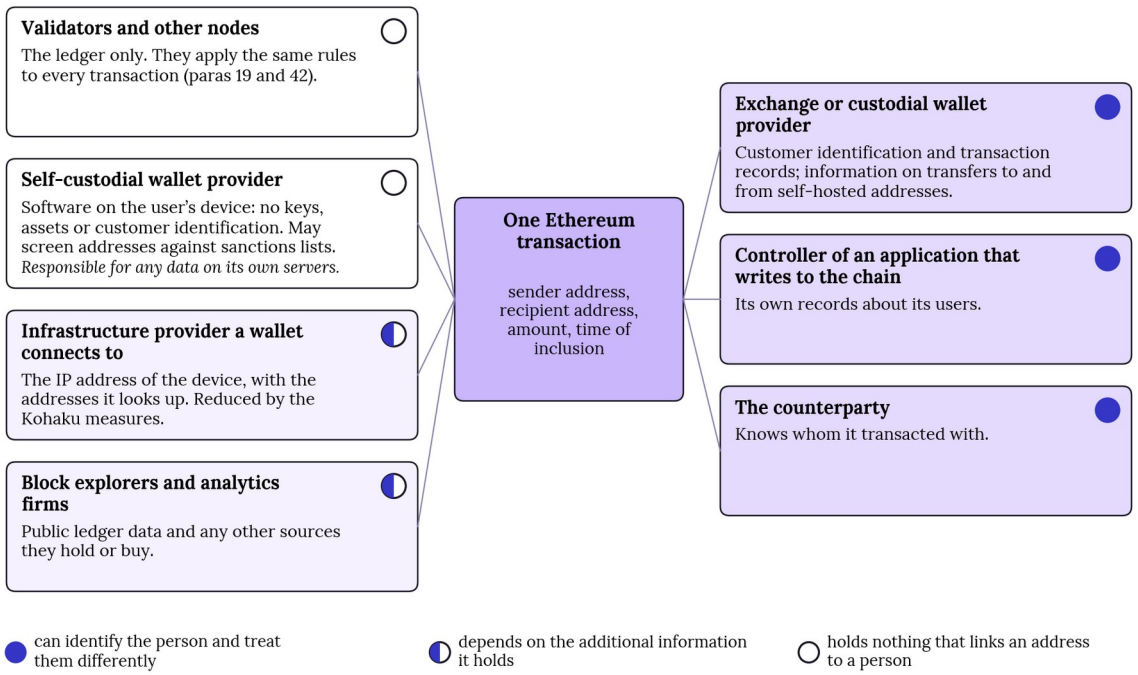


Figure 2. Who can identify the person behind a single Ethereum transaction, entity by entity.

Two consequences follow:

The first is that a node operator holding only the ledger, with no lawful or realistic access to anyone's identification records, does not identify anyone, provided paragraph 21 is not read as making every relay of public data personal for the relaying entity (Sections 8 and 9). The second is that the same analysis cannot make published transaction data anonymous as such, because some readers of the ledger, such as exchanges holding customer records, can link addresses to people, and paragraph 96 recalls that the goal of anonymisation is anonymity for all relevant entities. **EEI's main proposal therefore does not rely on the entity-by-entity argument. It rests on a construction in which nothing on the chain carries information about the person.**

3. EEI's main proposal: a perfectly hiding commitment whose witness has been deleted is anonymous

EEI proposes that the final text of the anonymisation guidelines state that **a commitment computed under a perfectly hiding scheme, whose input data and witness have been deleted, is anonymous information within the meaning of Recital 26 GDPR**, provided the conditions in Section 4 are met.

The proposal takes the Board's own description in paragraph 53 of the blockchain guidelines and applies the Board's own test to it, as Figure 3 shows. The commitment is a unique value, so No Record Isolation is not met. It cannot be used to single anyone out, because once the data and witness are gone there is nothing to match it against; in the words of paragraph 53, the original data can be neither recovered nor recognised, which is the situation paragraph 99 describes. A perfectly hiding commitment reveals nothing about its input, even to an attacker with unlimited computing power, so no inference

about the person can be drawn from it, and once no copy of the data and witness remains there is nothing to link it to. Since only a copy of the data and witness could connect it to a person, the result does not depend on the capabilities of any other entity, and once no such copy remains anywhere, the commitment passes even the simplified approach, which under paragraph 49 asks whether re-identification is possible in theory. Where a copy legitimately remains, for example with the data subject or a supervisor, the assessment is contextual, as Section 4 explains.

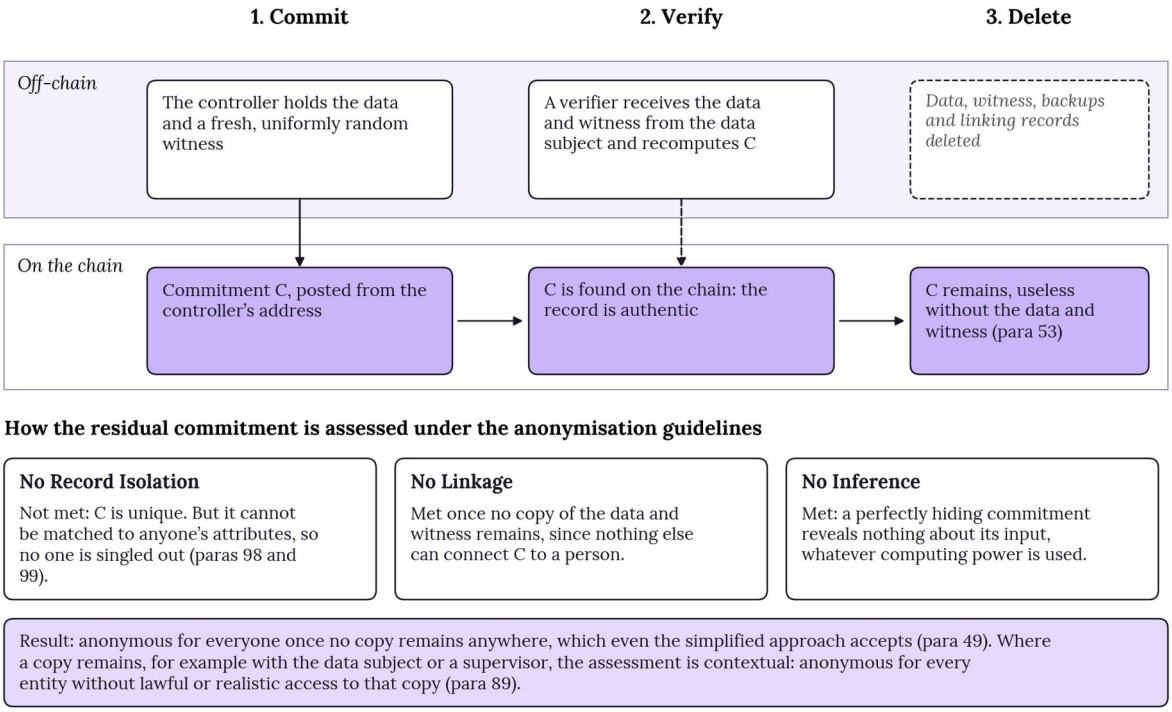


Figure 3. The lifecycle of a perfectly hiding commitment, and how the commitment left on the chain is assessed under the anonymisation guidelines.

The proposal is narrower than requests the Board has already declined. The consultation outcome report on the blockchain guidelines rejected requests to recognise specific cryptographic approaches as fully compliant solutions.[4] This proposal leaves the processing before deletion fully subject to the GDPR and concerns only the legal status of what remains afterwards. It does not cover encryption or hashes, which the blockchain guidelines (paras 51 and 52) and the anonymisation guidelines (para 91) keep within the GDPR, including the keyed hashes that real systems often publish next to their commitments (Sections 5 and 6), and it leaves addresses and the transaction graph where the blockchain guidelines put them. It is also narrower than EEI's own earlier positions. Our June 2025 response asked the Board to recognise deletion of the verifying key, witness value or decryption capability as functional erasure under Article 17, and our December 2025 answers argued that an actor receiving only zero-knowledge proofs, commitments or encrypted payloads, without access to the underlying attributes, should

[4] European Data Protection Board, Report on Public Consultation: Guidelines 02/2025 on processing of personal data through blockchain technologies, July 2026, section 3.

be considered to hold effectively anonymous data.[5] The present proposal keeps only the case where the Board's own text already describes the result.

Stating the result expressly would give paragraph 53 the legal qualification it currently lacks, and would give controllers one clearly defined way of meeting the requirement to delete or render data anonymous, without asking the anonymisation guidelines to rule on erasure itself, which paragraph 10 places outside their scope.

An example of a university that wants employers to be able to check its diplomas shows how this works: the university keeps each diploma record in its own systems, computes a commitment with a fresh witness, gives the graduate the record and the witness, and posts the commitment to Ethereum from its own address. An employer who receives the record and witness from the graduate recomputes the commitment and checks that it is on the chain. When the retention period ends, or the graduate asks for erasure, the university deletes its copies. The commitment stays on the chain, where it continues to support the integrity of the ledger as paragraph 64 of the blockchain guidelines anticipates, but nobody without a copy of the record and witness can match it to the graduate. Any copy the graduate or an employer keeps is additional information that the assessment has to take into account, which is why the conditions in Section 4 matter.

4. Technical conditions

A commitment scheme has two properties (blockchain guidelines, para 34): it is **binding** if the person who made the commitment cannot later open it to a different value, and **hiding** if the commitment reveals nothing about the value until it is opened. Hiding can be computational, meaning that breaking it would take more computing power than is realistically available, or perfect, meaning that the commitment carries no information about the value at all, so that every possible value is equally consistent with it. No scheme can be both perfectly hiding and perfectly binding, so a perfectly hiding scheme can only be computationally binding.

Further, paragraph 34 of the blockchain guidelines speaks of commitments applied correctly, and paragraph 53 of a state-of-the-art scheme. In practice, this means conditions that a controller can document and a supervisory authority can audit. The witness must be fresh for every commitment and drawn uniformly at random over the full range the scheme requires. Reusing it, or deriving it from the data, destroys the hiding property, and a witness derived from a key is only as hiding as the key. The public parameters of the scheme must be generated so that nobody knows the mathematical relationship between them, for example by deriving them from a fixed domain string, since anyone who knew the relationship could open commitments to other values; importantly, this affects binding, not hiding.

[5] EUCI, Response to EDPB Guidelines 02/2025, with co-signatories, June 2025; EUCI, Answers to the EDPB Discussion Questions for the event on Anonymisation & Pseudonymisation, 12 December 2025, answer to Question 4.

The input data and witness must be held off-chain under the controller's responsibility, and on erasure every copy must be deleted, including copies kept to rebuild a register, backups and copies held by processors. In practice this means keeping keys and records per data subject and letting backups expire on a schedule, since a key or a backup that covers all data subjects cannot be deleted for one of them. Copies held by the data subject, by verifiers to whom the commitment was opened, by a counterparty that created the data for the data subject, or by supervisors and auditors that received it in a disclosure, and any record that ties the commitment to the person, are additional information. Copies given to supervisors follow those authorities' own retention rules and remain outside any design. Where such copies remain, the assessment is contextual: the commitment is anonymous for every entity that has no lawful or realistic access to them, and data kept under appropriate security controls counts as accessible only to authorised users (anonymisation guidelines, para 89).

Nothing else in the transaction may tie the commitment to the person. It should be posted from the controller's address and not the data subject's, and any value that enters or leaves the system, such as a deposit or a withdrawal, should also pass through the controller, since a transaction sent from the data subject's own address shows that address next to the commitment it creates. The transaction should carry no other personal data. Other values that a system publishes next to its commitments, such as the identifiers that prevent a holding from being spent twice, are often keyed or salted hashes. They are in the position paragraph 52 of the blockchain guidelines describes and are not covered by the proposal (Section 6). Finally, the time and pattern of posting must not reveal whose commitment it is (anonymisation guidelines, para 79, on membership inference), which in practice means posting commitments in batches at fixed times rather than one at a moment that points to a single person.

Furthermore, we are not aware of a European or international standard that specifies how perfectly hiding commitments should be implemented and audited for data protection purposes, or how much batching is enough. EEI would welcome the Board setting out the state-of-the-art criteria it expects, with ENISA where appropriate, so that controllers and supervisory authorities apply paragraph 53 consistently.

5. Institutional example 1: a bank issuing a tokenised bond on Ethereum

Financial institutions already use public Ethereum for regulated activity. In April 2021 the European Investment Bank issued a EUR 100 million two-year digital bond on the Ethereum mainnet with Goldman Sachs, Santander and Societe Generale, and the payment from the underwriters was represented on the chain as central bank digital currency issued by the Banque de France.[6] On 21 September 2026 the Eurosystem launched Pontes, which links DLT platforms to TARGET Services so that wholesale

[6] European Investment Bank, press release 2021-141, European Investment Bank (EIB) issues its first ever digital bond on a public blockchain, April 2021; Consensys, press release of 29 April 2021 on the EUR 100 million two-year bond issued on the Ethereum mainnet.

transactions in tokenised assets can be settled in central bank money.[7] The difficulty institutions have so far raised is the transparency of the ledger: a token issued under the ordinary standard shows who holds what, every transfer and every counterparty, which EthSystems describes as a dealbreaker for institutions. In January 2026, the team published a proof of concept for private zero-coupon bonds, developed from the requirements of a major European bank, in which the bond contract stores only commitments to individual holdings and identifiers of spent holdings, while the issuer keeps a full audit trail for its regulators.[8]

Much of this activity takes place between institutions, and data concerning legal persons as such falls outside the GDPR (Recital 14). The GDPR becomes relevant when a bank serves natural persons, for example when it distributes a tokenised bond to its retail clients. Figure 4 shows how such a product can be built so that the bank meets its anti-money laundering retention obligations and then reaches a point at which the holdings recorded on the chain no longer relate to its clients.

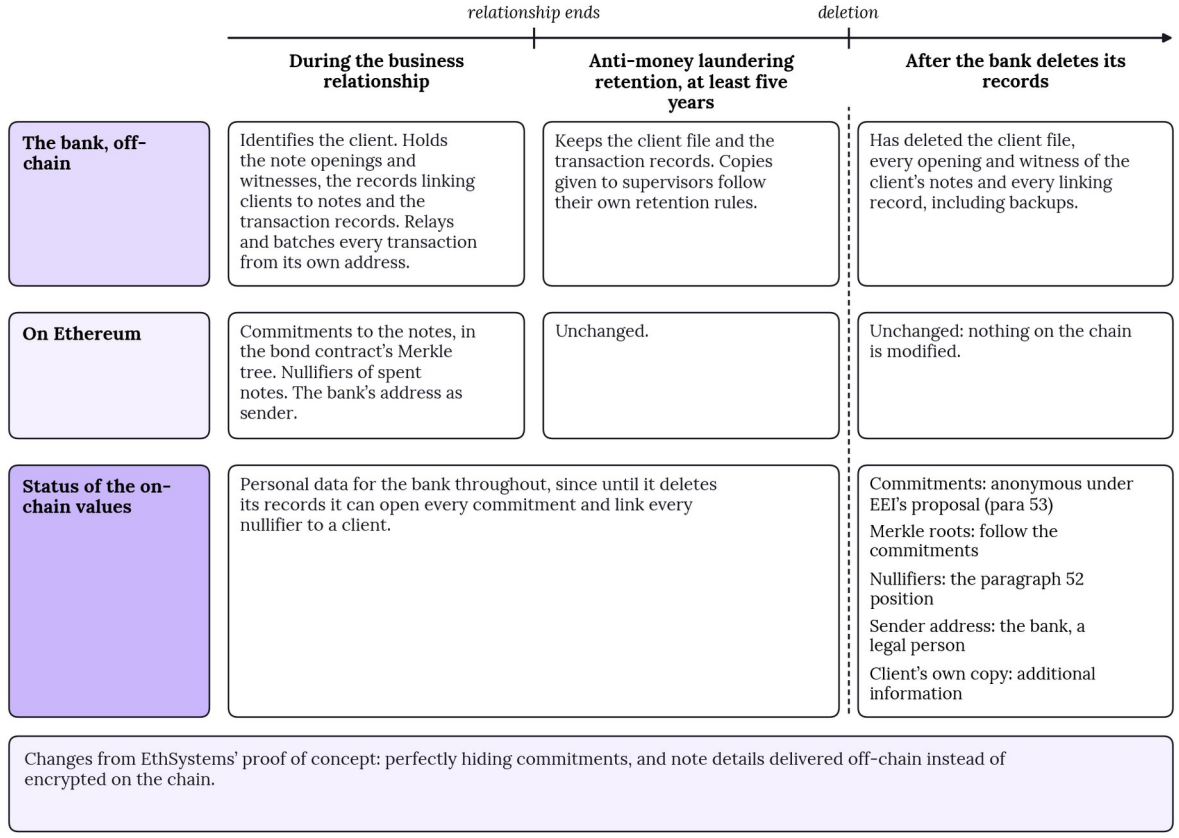


Figure 4. A tokenised bond distributed to retail clients on Ethereum: what the bank holds, what is on the chain, and the legal status of the commitments over time. EEI illustration, adapted from EthSystems' private bond proof of concept with the changes described in this section.

The bank identifies each client off-chain under its anti-money laundering obligations. Each holding is represented as a note, a record of the amount, the bond and its maturity,

[7] European Central Bank, press release, Eurosystem brings central bank money to tokenised finance, 21 September 2026.

[8] EthSystems, Building Private Bonds on Ethereum, 21 January 2026, https://ethsystems.org/writeups/building-private-bonds-on-ethereum/.

together with a random blinding value, and only a commitment to the note is placed on the chain, in a Merkle tree kept by the bond contract. The bank acts as relayer, submitting all transactions from its own address and batching them as Section 4 describes, so that neither the sender nor the time of posting points to a particular client. When a client sells or redeems a holding, a zero-knowledge proof shows that the client holds a valid note and that the amounts balance, without revealing the note, and a nullifier, an identifier derived from the note's secret values, is published so that the same note cannot be spent twice. The bank holds the openings of all notes and can reconstruct each client's position for its supervisors.

Two features of this design go beyond the proof of concept, and both are needed for the proposal in Section 3 to apply. First, the proof of concept computes note commitments with a hash function, which is only computationally hiding; here the commitments must use a perfectly hiding scheme. Second, the proof of concept places encrypted copies of the note details on the chain, so that holders can recover them if the issuer disappears. For natural persons, encrypted personal data on the chain remains personal data and will be overtaken by time (blockchain guidelines, para 51), so these details should be delivered off-chain, with the bank taking responsibility for their availability.

The bank keeps the client file and the transaction records for as long as anti-money laundering law requires, at least five years after the end of the business relationship (blockchain guidelines, footnote 43), and then deletes them, together with every opening of the client's notes and every record linking the client to a note. From that point, the commitments on the chain meet the conditions in Section 3: they are unique values that cannot be matched to anyone and carry no information about the client. The address from which they were posted belongs to the bank, a legal person, and the Merkle roots are computed from the commitments and add nothing to them. The nullifiers are in a different position: they are not commitments but hash values derived from the note's secret values and a key the client holds, so anyone who still has that key, such as the client's own wallet, can link each spend to its note, and without it the link rests on the strength of the hash function, which is the position paragraph 52 describes. The proposal does not cover them, as any note data the client keeps in their own wallet remains additional information in the client's hands, as in the diploma example.

If the final text confirmed, as EEI proposes in Section 3, that a perfectly hiding commitment is anonymous once its input data and witness have been deleted, the bank could record in its data protection impact assessment, with legal certainty, that the commitments it leaves on the chain cease to be personal data when the retention period ends. Without it, the bank cannot say what the on-chain record becomes once the retention period ends, while the blockchain guidelines require a technical solution that allows deletion or anonymisation at the end of the retention period, and otherwise no personal data on the chain (Recommendation 11), and ask organisations to favour permissioned chains unless well-justified reasons hinder that preference (para 40). With it, the bank can document an end state that it reaches by deleting data it controls, without

relying on the nodes or on any change to the chain, and can assess the remaining values, such as the nullifiers, under paragraph 52. **Responsibility remains with the bank, which knows its clients and can treat them differently**, and once deletion has taken place, the nodes, including other institutions that run nodes, hold commitments that are no longer personal data for anyone.

6. Institutional example 2: a money market fund, with the bank as transfer agent

Tokenised money market funds on Ethereum today run as tokens that only approved addresses can hold, with holdings, subscriptions, redemptions and yield visible to anyone. EthSystems' design for confidential fund shares, published as a draft specification in October 2026, moves the confidential holdings into a pool that holds the fund's public token on their behalf.[9] It is built around a role that already exists in fund administration: the **transfer agent**, the intermediary that keeps the fund's register. The transfer agent confirms each subscriber's cash off-chain, deposits the day's total into the pool from its own address and hands out the holdings as notes through ordinary shielded transfers. A holder redeems by transferring a note back to the agent, which withdraws the day's total and pays the cash off-chain. The agent also attests, through a registry, which pseudonymous owner keys are eligible to hold notes, while the link between those keys and investor identities stays in its own records, and it can freeze or seize a note through a separate path. The design's own requirements state that no personal data goes on the chain, even in encrypted form.

For data protection, the value of this design lies in the proposed middleman: every link between the chain and a person runs through the transfer agent, which identifies the client, holds the keys and the mapping from pseudonymous keys to investors, and in a retail version it would be the only party that posts to the chain. The rest of the network sees the agent's address, daily aggregates and commitments. **The entity that knows the clients and can treat them differently in the sense of paragraph 19 is therefore the one that holds the additional information and decides when it is deleted**.

The fund was designed for institutional holders, most of which are legal persons outside the GDPR (Recital 14). A bank that offered it to retail clients, acting as transfer agent and as the only relayer, would likely need four changes to the design for the proposal in Section 3 to apply:

First, the copies of each note are delivered off-chain. As specified, the fund places every new note on the chain twice in encrypted form: once for the holder, so that the holder's wallet can find it, and once for the transfer agent's register, so that the register can be rebuilt from the chain. Each copy shows how much a holder has, next to a pseudonymous key that the agent links to the holder's identity. For an institution, this is not personal data, which is how the design meets its own requirement that no personal data goes on

[9] EthSystems, Shielded Notes: Private Money Market Fund Shares, protocol specification, version 0.1.0 (draft), 6 October 2026, https://github.com/ethsystems/pocs/blob/master/pocs/private-mmf/shielded-notes/SPEC.md; EthSystems, Building Private Money Market Funds on Ethereum, 23 October 2026, https://ethsystems.org/writeups/building-private-money-market-funds-on-ethereum/.

the chain; for a natural person, it is, and encryption does not change that (blockchain guidelines, para 51). In the adapted design, the bank delivers both copies off-chain, and only a hash of each is bound to the proof, so that the contract can still check that the copies match the note.

Second, the bank can delete one client's data without affecting the others'. As specified, every copy for the register is encrypted to a single register key that covers all holders. While those copies stay on the chain, deleting one client's records achieves little: the bank could restore them by decrypting the chain again, rotating the key protects only later notes, and deleting the key would end the agent's ability to rebuild the register for everyone. Once the copies are off-chain, two further changes make deletion for one client possible: the daily checkpoint that the agent publishes, today a single salted hash over the whole register, becomes a root over one salted hash per client, so that one client's row can be removed while the checkpoint still holds for the others. And the bank keeps keys and records per client, with backups that expire on a schedule, rather than any key or backup that covers every client. The contract itself does not need to change.

Third, the note commitments become perfectly hiding. The fund computes them as salted hashes, which are only computationally hiding. In the adapted design, they are Pedersen commitments over a curve the proof system can work with efficiently, such as the Grumpkin curve, with a blinding value drawn over the full group order and generators derived from a fixed domain string, as Section 4 describes. The commitment tree, the formula for nullifiers and the agent's ability to open and claim any note can stay as they are. The cost of the change still has to be measured against the specification's figures for a transfer today, about 2.4 seconds of proving and 3.2 million gas.

Fourth, clients' own addresses stay off the chain. Transfers go only to the client's own notes and to the bank, and the bank makes all deposits and withdrawals, as the transfer agent already does for subscriptions and redemptions. The bank also posts in batches, as Section 4 describes. The fund already batches its daily issuance and redemption, and its registry of eligible owner keys already publishes in padded batches of at least 16, but transfers are submitted as they arrive.

The bank keeps the client file and the transaction records for as long as anti-money laundering law requires, and then deletes them, together with the client's keys, every opening of the client's notes and every record linking the client to a note.

Two conclusions follow. The commitments reach the position that EEI's proposal addresses, provided the conditions in Section 4 are met. Most of the other values, the nullifiers in particular, reach the position paragraph 52 of the blockchain guidelines describes: the Board accepts that a keyed or salted hash should no longer be linkable once its key or salt is deleted, but neither text qualifies such a hash under the anonymisation guidelines, a gap Section 9 returns to. Bringing the nullifiers into the position of paragraph 53 would mean deriving them from a fresh secret held inside the perfectly hiding commitment, a change that has not yet been designed. Public totals and timing, finally, depend on how the product is operated rather than on its cryptography.

Importantly, the same approach can be applied to other institutional uses, such as payments and stablecoin settlement, but each needs its own analysis of what it publishes.

7. Trade-offs, and why they are decided when each use case is modelled

The examples in Sections 3, 5 and 6 are prototypes. They show that systems built on public Ethereum can be designed so that a controller meets its sectoral obligations and then reaches an end state the blockchain guidelines accept, and they make concrete what the Board's texts require of such a design. They are not the only possible designs, and none of them is a finished product.

Nevertheless, it is important to note that every choice that brings a system closer to deletion or anonymity gives something else up. The GDPR already expects controllers to make these choices at the design stage. Article 25(1) requires appropriate technical and organisational measures, decided at the time the means of processing are determined and taking into account the state of the art, the cost of implementation, the nature, scope, context and purposes of the processing, and its risks, and the impact assessment under Article 35 is where the choices and their reasons are recorded. **The right balance for a fund held by retail clients will not be the right balance for a diploma register or a payment system**, so these choices can only be made when a given use case is modelled.

The central trade-off is between retention and availability. Anti-money laundering law requires the bank to keep its records for at least five years after the business relationship ends, data protection law requires them to be deleted or anonymised once that period is over, and throughout, clients and the market need positions to be available and recoverable. Placing the note details on the chain in encrypted form secures availability without depending on the bank: a holder whose wallet has lost its notes, or a successor transfer agent, can rebuild positions from the chain with a key, and where the on-chain ledger is part of the official register of ownership, the chain alone determines positions. But it keeps encrypted personal data on the chain and, where one key covers all holders, makes deletion for a single client impossible. Delivering the details off-chain makes deletion possible, and the price is paid in availability. The bank's store becomes the only copy and has to meet the bank's usual availability and backup standards, while its backups have to expire on a schedule for deletion to be real. Wallets no longer find their notes by scanning the chain, so the bank has to deliver them, for retail clients most likely through its app. And since a hash proves that a copy is correct but not that the bank received it, the bank has to be in the path of every transaction, either as the only relayer or through a contract that checks the bank's signature over each hash. For a bank this is ordinary record-keeping, and it already carries the responsibility; for other controllers it may be a heavier burden.

These examples concern a controller that chooses to record information about its clients on a public chain. They are not a template for other uses: nothing in this response suggests that people who transact from their own addresses, peer to peer or through

decentralised applications, or the crypto-asset service providers and wallets that serve them, must adopt the same design, and the position of those uses is not addressed here.

This is why EEI does not ask the Board to approve particular designs. What controllers need is legal certainty about the end state they can reach, so that the trade-offs can be weighed when each use case is modelled against a known legal outcome.

8. The protocol layer, and expected Ethereum developments

The definition of identification in paragraph 19 has a direct bearing on the base layer. A validator applies the same rules to every transaction: it checks signatures, nonces and balances, executes the code the transaction calls and records the result. In that role, it has no relationship with the people behind the addresses, provides them with no service and takes no decision concerning them; an entity that runs validators and also holds customer records, such as an exchange, is assessed on all the means it holds. The blockchain guidelines take a similar view, as nodes whose role is limited to preparing the transactions to be included in the next block, without particular interest or benefit resulting from choosing specific transactions, and to a simple verification of technical validity, might not be controllers (para 42). Where the Board considers that nodes may be controllers, it is because they can exercise a decisive influence on the transactions added to the next block, or jointly decide on changes to the protocol (para 44).

The inclusion and ordering of transactions are therefore the points at which a protocol-layer actor could treat one transaction, and through it one person, differently from another, and Ethereum's next two upgrades change how they are decided. Glamsterdam brings the separation between block proposers and block builders into the consensus protocol (EIP-7732): the proposer includes a builder's signed bid for the block, and the builder reveals the block's contents afterwards. Glamsterdam activated on the Sepolia test network on 6 October 2026, and the Ethereum Foundation's protocol team plans to ship it on mainnet in December 2026.[10] Fork-choice enforced inclusion lists (FOCIL, EIP-7805) would allow a committee of sixteen validators in each slot to publish lists of transactions from the public mempool, and attesters would vote only for a block that includes them, unless the block is full or a listed transaction can no longer be validly added. The mechanism works as intended if a single member of the committee is honest, and it covers transactions in the public mempool rather than those sent privately to a builder.[11] FOCIL and Frame Transactions (EIP-8141) are the two proposals scheduled for inclusion in the following upgrade, Hegotá, which has no date yet, and the Foundation's

[10] EIP-7773, Hardfork Meta: Glamsterdam, activation table, https://eips.ethereum.org/EIPS/eip-7773; Ethereum Foundation Blog, Glamsterdam Hoodi Testnet Announcement, 16 October 2026, https://blog.ethereum.org/2026/10/16/glamsterdam-hoodi-announcement; Ethereum Foundation Protocol Cluster, EF Protocol: Current and Emerging Priorities, 7 September 2026, https://blog.ethereum.org/2026/09/07/protocol-priorities.

[11] EIP-7805, Fork-choice enforced Inclusion Lists (FOCIL), Draft, https://eips.ethereum.org/EIPS/eip-7805, sections on roles and participants and on core properties; EthSystems, Ethereum Upgrades: Past, Future, and Coming soon, 19 October 2026, https://ethsystems.org/writeups/ethereum-upgrades-past-future-and-coming-soon/.

protocol team has made them the upgrade's headliners, to ship together.[12] Once FOCIL is active, a block that left out a listed transaction without such a reason could not become part of the canonical chain. Builders will still decide the order of transactions.

These changes concern the role of protocol-layer actors and do not make any on-chain data anonymous; nothing scheduled for Glamsterdam or Hegotá hides a transaction from the services that relay it or from anyone reading the chain.[13] The developments that reduce identifiability are taking place in the access and ecosystem layer and in applications, as Figure 5 shows. The Ethereum Foundation's Kohaku roadmap for wallets provides for a light client that removes the need to trust remote servers for the validity of the data a wallet reads, state queries to servers that cannot see which data is requested, measures against unnecessary leakage of IP addresses, a default prompt to use a new address for each application, and the optional broadcast of transactions directly to the peer-to-peer network.[14] Each of these reduces the additional information that the services a wallet connects to can collect, which the anonymisation guidelines treat as decisive for identifiability (paras 20, 29 and 30), and separate addresses for separate applications remove a common identifier through which records are often linked (para 62).

Furthermore, the Ethereum Foundation's mandate, published in March 2026, commits the Foundation to treating censorship resistance, open source, privacy and security as the precondition of Ethereum's development priorities.[15] The roadmap also prepares for quantum computing: the Foundation's protocol team aims for Ethereum to be quantum-resistant across its execution, consensus and data layers by December 2029. Kohaku's published tooling already includes a post-quantum account implementation. These changes may be seen as the planned algorithm change the blockchain guidelines ask for (paras 85 and 114).

On this reading, a validator that holds only the ledger and applies the protocol's rules uniformly is not in a position to identify anyone within the meaning of paragraph 19, and the transaction data it processes is not personal data from its perspective (paras 6, 7 and 22). The obligations of the GDPR then fall on the entities that can identify people and act on that identification: the controller in the application layer and, for their own records, the crypto-asset service providers in the ecosystem layer, including exchanges and custodial wallet providers, which the law already requires to know their customers. The provider of a self-custodial wallet is in a different position. It is responsible for the data it processes itself, such as the IP addresses that reach its servers together with the addresses a wallet looks up, which can link an address to a connection, and the Kohaku

[12] EIP-8081, Hardfork Meta: Hegotá, Draft, https://eips.ethereum.org/EIPS/eip-8081; EF Protocol: Current and Emerging Priorities (cited above), section V.

[13] EthSystems, Ethereum Upgrades (cited above), section on who can read a transaction.

[14] Ethereum Foundation, Kohaku Roadmap, https://notes.ethereum.org/@niard/KohakuRoadmap; Ethereum Foundation Blog, The Ethereum Foundation's Commitment to Privacy, 8 October 2025, https://blog.ethereum.org/2025/10/08/privacy-commitment.

[15] Ethereum Foundation, The Ethereum Foundation Mandate, 13 March 2026, https://ethereum.org/foundation/mandate/.

measures described above reduce exactly that data. For the ledger, it holds no identification records and, like a validator, is assessed on its own means (anonymisation guidelines, paras 6, 7 and 20), so the reasoning on Article 11 set out below applies to it as well.

If the Board nevertheless decides to treat validators as processing personal data, for example through a broad reading of paragraph 21, that would not in itself make them controllers: the blockchain guidelines accept that nodes whose role is limited to a simple verification of technical validity might not be controllers (para 42). Even if a validator were treated as a controller, the result would show exactly why the obligations do not fit at that layer: a validator has no contact with the people behind the addresses and could not inform them under Articles 13 and 14; further, it could not rectify or erase a record unless the other nodes agreed to change the chain (blockchain guidelines, para 50). It could act on an objection under Article 21 only by keeping that person's transactions out of the chain, which is what FOCIL is designed to prevent. The GDPR already addresses a controller in this position: under Article 11, a controller whose purposes do not require the identification of data subjects is not obliged to acquire additional information in order to identify them, and where it can demonstrate that it cannot identify them, the rights in Articles 15 to 20, including rectification and erasure, do not apply unless the data subject provides information enabling identification.

In the consultation on the blockchain guidelines, the Board rejected proposals to exempt public blockchain architectures from the GDPR on account of their decentralisation, and EEI does not ask for that.[16] The argument here rests on the Board's own definition of identification in paragraph 19 and on its own criteria for when nodes are controllers in paragraphs 42 and 44.

[16] European Data Protection Board, Report on Public Consultation (cited in Section 3), section 3.

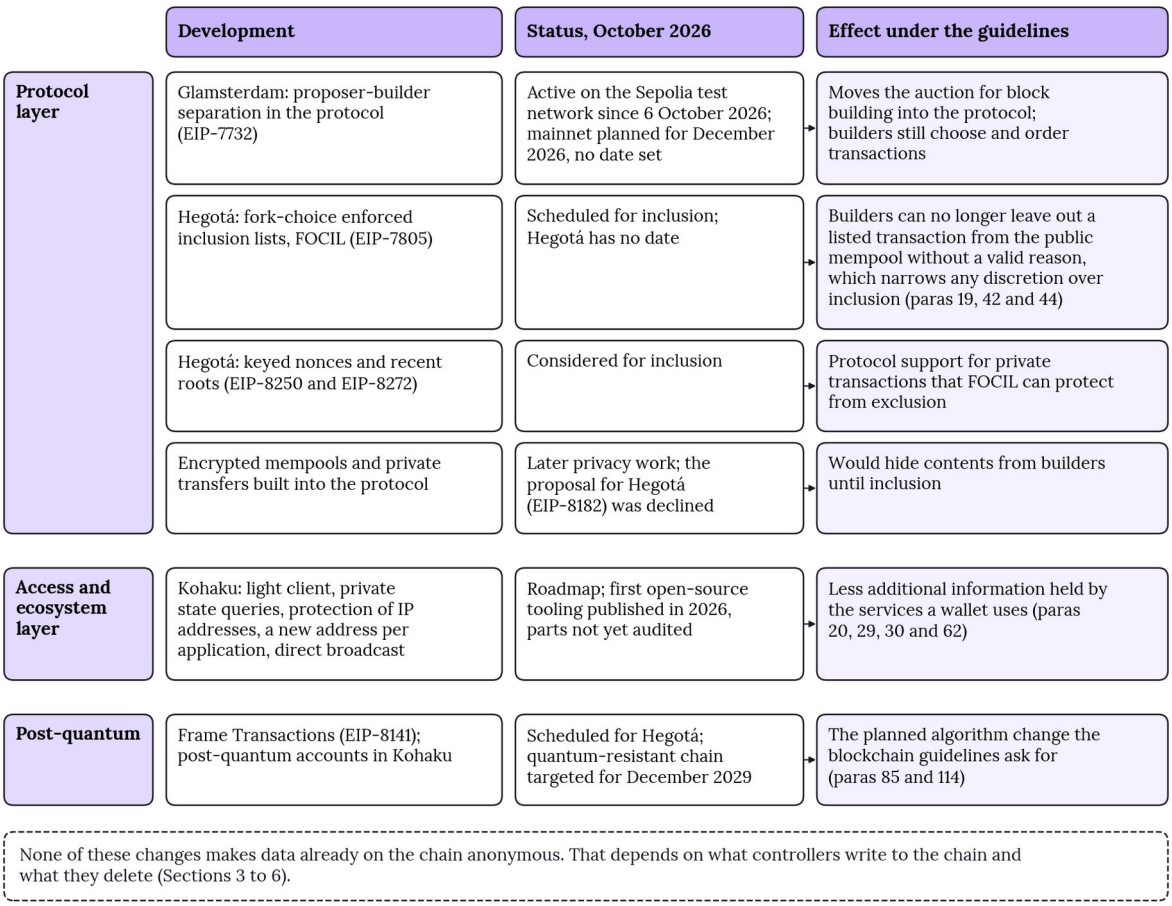


Figure 5. Expected Ethereum developments and their effect on identifiability under the guidelines.

9. What needs to be clarified and aligned

Guidelines 02/2025 on blockchain technologies and Guidelines 02/2026 on Anonymisation were adopted at the same plenary, on 7 July 2026, but neither refers to the other. Therefore, several points need to be settled if controllers are to rely on them:

The status of the residual commitment. Paragraph 53 of the blockchain guidelines describes the result of deleting the data and witness but not its legal status, and the anonymisation guidelines do not mention commitments. One sentence in either text, along the lines of the proposal in Section 3, would close the gap.

The meaning of "rendered anonymous". The blockchain guidelines rely on rendering data anonymous repeatedly (paras 60, 64, 71, 80 and 103, and Recommendations 9, 11 and 16) without saying which standard applies. The texts should state that it is the standard in the anonymisation guidelines. They also need to be reconciled on substance. Paragraph 103 of the blockchain guidelines presents erasure of off-chain data as what renders on-chain data anonymous, whereas the anonymisation guidelines assess anonymity against every relevant entity, including those holding their own additional information (paras 11, 20 and 29). For data such as addresses, erasing one controller's records does not touch what an exchange holds under its own retention obligations. The Board should make clear which designs meet both texts. The same question arises for the values that complete

designs publish next to their commitments. Paragraph 52 of the blockchain guidelines accepts that a keyed or salted hash should no longer be linkable once the key or salt is deleted, provided the algorithm holds and nothing has leaked, but neither text says whether such a hash is then anonymous under the anonymisation guidelines. In both institutional designs examined in Sections 5 and 6, the identifiers that prevent double spending are in this position, so the answer decides whether such designs can reach the end state the blockchain guidelines ask for, including for an institution that can only begin deleting once its anti-money laundering retention period has ended.

Node operators. The anonymisation guidelines assess an entity that processes data on behalf of a controller from the controller's perspective (para 15). The blockchain guidelines accept that in certain cases nodes on public permissionless chains do not act on behalf of any controller, and that nodes with limited decision-making power might not be controllers (paras 42 and 44). The Board should confirm that such nodes are assessed from their own perspective; that applying the protocol's uniform rules, without discretion over which transactions are included, does not put a node in a position to treat anyone differently in the sense of paragraph 19; and that customer records held by exchanges under security controls, to which a node has no lawful access, are not a means reasonably likely to be used by that node (anonymisation guidelines, paras 26 and 89).

The same reasoning applies to providers of self-custodial wallet software and operators of interfaces to decentralised applications, which hold no identification records about their users. The Board should confirm that they too are assessed on their own means, and that screening addresses against sanctions lists, which does not require knowing who the user is, does not by itself put them in a position to identify anyone.

Publication and relay. Paragraph 21 draws on the Court's reasoning in *EDPS v SRB* about a transfer to an identified recipient (footnotes 17 and 18). Read literally, it would make any data published on a public ledger personal for every node that relays it, whatever that node's own means, because it can never be ruled out that some reader can identify the person. That would leave little of paragraphs 6, 7 and 22 for public data. The Board should explain how paragraph 21 applies to publication and relay.

Periodic reassessment of data that cannot be changed. The anonymisation guidelines recommend periodic reassessment because re-identification becomes easier over time (para 35 and footnote 3), and the blockchain guidelines ask for periodic reassessment of encryption and note that the impact assessment may need to be an ongoing process for permissionless chains (paras 96 and 99). For ledger data, the outcome of a reassessment cannot be acted on by changing the data. The hiding property of a perfectly hiding commitment does not weaken with time, computing power or AI. Even a quantum computer able to break the discrete logarithm problem would allow someone to open such a commitment to a different value, which is a question of integrity, but would not reveal what it was computed from. Reassessment can therefore concentrate on whether a copy of the data and witness, or a record linking the commitment to a person, has resurfaced. Either text should recognise this.

Continuing the work. EEI intends to stay engaged with the Board until the final text is adopted. We would welcome the opportunity to bring together controllers, crypto-asset service providers, wallet and protocol developers and the teams building designs such as those discussed here, in order to map, actor by actor, how anti-money laundering obligations and the GDPR's requirements on deletion and anonymisation fit together in concrete systems.

About the European Ethereum Institute

The European Ethereum Institute (EEI, formerly the European Crypto Initiative) is a Brussels-based non-profit advocacy organisation. It supports fair, innovation-friendly regulation for decentralised technology and promotes Ethereum as public infrastructure for Europe's digital and financial environment. We have contributed to the Board's work on blockchain and anonymisation since the consultation on the blockchain guidelines in 2025, and we would welcome the chance to discuss these points or to provide specific drafting.

Website: ethereum.institute **Contact:** contact@ethereum.institute