SCIENTIFIC BLOCKCHAIN ALLIANCE · GENERAL ASSEMBLY, GENEVA

Hashes, proofs, the notion of personal data and the Digital Omnibus

Why decentralised verification might be at risk after the Digital Omnibus

Dr. Jörn Erbguth

Scientific Blockchain Alliance · October 2026

UNIVERSITÉ DE GENÈVE

SCIENTIFIC BLOCKCHAIN ALLIANCE

THE POLICY TRACK

From EDPS v SRB to the Digital Omnibus

4 Sep 2025

CJEU, EDPS v SRB (C-413/23 P)

Identifiability is assessed from the recipient's perspective; means are not "reasonably likely" if identification is impossible, disproportionate or prohibited (para. 82). The EDPB had read Breyer the other way.

19 Nov 2025

Commission: Digital Omnibus

Three sentences added to Art. 4(1): data are not personal for an entity that cannot identify – a purely relative definition. Plus Commission implementing acts with technical criteria.

7 Jul 2026

EDPB guidelines

Blockchain v2.0 (para. 52: a hash stays personal data) and draft Guidelines 02/2026 on anonymisation (processor and third-party restrictions).

3 / 21 Sep 2026

Council: ST 12535/26, ST 13112/26

Art. 4(1) change dropped. New Art. 25a for pseudonymised data only, EDPB opinion instead of implementing acts, transmission and processor rules.

THE ORIGINAL PROPOSAL

Would hashes become non-personal for node operators?

Under the Commission text: yes, for some

Node operators and observers cannot identify anyone from a hash – for them it would not have been personal data. Issuers and verifiers hold the document; for them nothing would have changed.

The risk the Council saw

Pseudonymised data leave the Union as “non-personal” for the exporter, are re-identified in a third country, outside GDPR enforcement. Chapter V never applies because the data were never personal for the sender.

The Council’s answer (Art. 25a, ST 12535/26; structure kept in the revised text of 21 September):

(2) pseudonymised data are not personal data only “for a person … unable to identify” – and only as long as it passes nothing on

(4) for processors the data remain personal; recital 27b: data become personal once at the disposal of persons with means

(5) transmission to a third party with means, and that party’s processing, “is processing of personal data”

THE STARTING POINT

Identifiability alone is not personal data

A calendar

Every date of birth of every living person is in it. Nobody would call a calendar personal data. The dates are there, the persons are not.

The list of all IPv4 addresses

2^{32} addresses, each one assigned to somebody at some time. The complete list is not personal data either, although every entry can be an identifier (Breyer, C-582/14).

The question is not “can somebody be identified?” but “when does identifiability turn a piece of data into personal data?”

THE DEFINITION

Art. 4(1): an identifier plus information about the person

Identifier

date of birth, IP address, hash, key …

→

Link

“relating to” – by content, purpose or effect (Nowak, C-434/16)

→

Information

about the person, and not already needed to form the identifier

Which information? Not the input of the identifier itself.

The date of birth is what the calendar entry is made of; it cannot at the same time be the information the entry links to. In the same way, the document that was hashed is the input of the hash, not information the hash adds. Personal data arises when additional information is attached to the identifier – information that is not contained in the hashed document.

A hash becomes personal data only if it links additional information to a person. Whether verifiability is such information: see next slide

VERIFICATION VS ENDORSEMENT

Is verifiability such information? Depends on the issuer

Endorsement

A third party states something about the document or the person: “this diploma is genuine”, “this holder is over 18”, “this account passed KYC”. That statement is new information from outside. The artefact that carries it relates to the person – it remains personal data.

Verification by the author

The author of the document issues, together with the document, the means to check that it is unchanged and existed at a given time. Nothing is added that the document does not already say. Whoever verifies must already hold the document – and is, for that document, already within the GDPR.

Verification adds no information about the person. Endorsement does.
The GDPR line runs between the two – not between mere identifiability.

WHY THE DISCRIMINATION IS VISIBLE

The centralised twin: the certificate behind a seal

Qualified seal (eIDAS Art. 36–38)	Document with personal data	→	Signature value – part of the document	→ Verifiable through the certificate → Certificate: public, not personal data
Qualified time stamp (eIDAS Art. 42)	Document with personal data	→	Hash – only the hash leaves the issuer	→ TSP signs hash + time → TSP certificate and records: public
Decentralised verification	Document with personal data	→	Hash (salted if needed)	→ Anchored with time and key → Ledger entry: public – personal data?

The signature value is part of the document and is treated as personal data together with it. What makes the document verifiable is the certificate – public, and not treated as personal data of the persons named in the documents it secures. The hash on the ledger plays exactly the role of the certificate; on the EDPB's reading it is personal data (Guidelines 02/2025 on blockchain, para. 52).

Certificate and ledger hash do the same job. Decentralised verification should not be discriminated against.

SALT AND PEPPER

Salt: needed only when the entropy is not enough

Low entropy

Name + date of birth, an e-mail address, an ID number: a few billion candidates at most. A hash of such data can be brute-forced, so the hash itself makes the person guessable – it is personal data.

Random salt

A random value per document, stored with the document, removes the guessability. A scanned diploma, a contract or a photo has enough entropy on its own and needs no salt; a form with a name and a date does.

Salt is a remedy for low entropy – nothing more.
Where the document cannot be guessed, the hash needs no salt.

SALT AND PEPPER

Pepper: a separate secret that helps nobody

What authorities ask for

A secret (“pepper”), kept apart from the data, so that the hash can later be rendered anonymous by deleting the secret.

Fine for an endorsement

Where a third party attests something and the artefact is not meant to be re-verified by everybody, a secret held by the endorser makes sense.

Pointless for verification

If the document is to be verifiable at all times, document and secret always travel together. No privacy is gained; usability is lost. The document itself already is the secret.

“Delete the secret to anonymise the hash” is not a safeguard. A secret that always travels with the document can be deleted exactly as well – or as badly – as the document itself. So it is not needed: the document already is the secret.

THE CONSEQUENCE

Whatever is built to be verified later stays personal data

Hash

The holder recomputes it from the document.

Commitment

Opened later with the committed value and randomness.

Zero-knowledge proof

Proves a statement about data the prover holds; the verifier learns that the statement is true about that data.

All of these are pseudonymisation: outsiders cannot identify anyone. Yet the relief in Art. 25a(2) lasts only as long as the outsider passes nothing on – and issuer, verifier and node are exactly the parties the text keeps within the GDPR.

Issuer / publisher	holds the document → personal data (unchanged by Art. 25a)
Verifier	receives the document, recomputes → processing of personal data (Art. 25a(5))
Node operator	cannot identify, but serves chain data to verifiers with means → transmission is processing of personal data (Art. 25a(5))

THE CONSEQUENCE

Not a blockchain problem: every hash-only service is affected

Trust services

Qualified time stamps (Art. 42 eIDAS) and remote signing (Art. 29a) receive only the hash of the document. The provider would process the data of every person in every stamped or signed document – Art. 28 contracts, erasure vs. retention, Chapter V.

EU Digital Identity Wallet

mdoc and SD-JWT credentials carry salted digests of every attribute; the relying party receives the digests of what is not disclosed. Status lists are distributed to everyone. Unlinkability is built on batch keys and zero-knowledge proofs – all verification artefacts.

Archives and logs

Evidence preservation and hash manifests, Merkle audit logs, backup deduplication by content hash, signed SBOMs and commit hashes with author identities, certificate-transparency logs with personal certificates, revocation lists at hosters and CDNs.

The same legislator wrote the Wallet’s data minimisation on the premise that salted digests are not personal data for the relying party. It cannot codify the opposite in the Omnibus.

PROPOSAL

What a rule for verification would have to say

> **“Data that serves only to verify other personal data, without adding to that data and without making it possible to guess it, should not be considered personal data.”**

Verification, not endorsement

Only artefacts that add nothing about the person. A statement from outside stays personal data.

Not guessable

Low-entropy inputs need a salt; otherwise the artefact itself is an identifier with information.

Parity with eIDAS

Same treatment as seal values, certificates and time-stamp records.

Where it belongs: in Article 25a itself or at least in recital 27b – the only places that bind the EDPB when it drafts the opinion foreseen in Article 25a(6). The public consultation before that opinion (recital 27c) is a fallback, not a strategy.

Takeaways

1 **Identifiability is not enough.**

Personal data need an identifier and information that relates to the person – the calendar and the IPv4 list prove the point.

2 **Verification adds no information.**

Issued by the author, the ledger hash does what the certificate behind a seal does – and certificates are not personal data. Endorsement is different.

3 **Salt only against low entropy, no pepper.**

A salt is needed where the document could be guessed. A secret that travels with the document adds nothing: the document already is the secret.

4 **The Omnibus does not reach us.**

Article 4(1) is gone; Article 25a relieves only a passive outsider who neither identifies nor forwards. Issuer, verifier and node stay within the GDPR.

Dr. Jörn Erbguth

joern@erbguth.net · erbguth.net · blockchain-gdpr.org

UNIVERSITÉ DE GENÈVE

SCIENTIFIC BLOCKCHAIN ALLIANCE

Sources

- CJEU, 4 September 2025, EDPS v SRB, C-413/23 P, paras. 77, 82, 86; CJEU, 19 October 2016, Breyer, C-582/14; CJEU, 20 December 2017, Nowak, C-434/16.
- European Commission, Proposal for a Regulation … (Digital Omnibus), COM(2025) 837, 19 November 2025, 2025/0360 (COD).
- Council of the EU, Presidency revised compromise text ST 12535/26 (3 September 2026; published by noyb.eu) and revised compromise text ST 13112/26 (21 September 2026; listed in meeting notice CM 4156/26). Paragraph numbers of Article 25a follow ST 12535/26.
- EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies, v2.0, 7 July 2026, para. 52; EDPB, Guidelines 02/2026 on anonymisation, v1.0 for public consultation, 7 July 2026, paras. 15, 20, 26, 28; EDPB–EDPS Joint Opinion 2/2026.
- Regulation (EU) No 910/2014 (eIDAS), Articles 36–38 (electronic seals), Article 42 (qualified electronic time stamps).
- J. Erbguth, Blockchain and the GDPR – Status Report for Blockchain for Europe, 3 December 2025, blockchain-gdpr.org; J. Erbguth, Proving What Is Real (policy note), September 2026.