Reliable Context

RELIABLE CONTEXT / RESEARCH & PRACTICAL GUIDANCE

GDPR Erasure and Rectification in Event-Sourced Systems

> Reliable Context is a kernel of truth: a system of record for organizations that fuse private and public information and must defend every value they act on. One canonical record per real thing, a cited source and an observation date behind every value, unknowns declared rather than left blank, and any past state of the record reproducible.

Published by Reliable Context · 2026-10-29 · gdpr event sourcing · gdpr right to erasure immutable · gdpr append only database · crypto shredding gdpr · gdpr article 16 rectification

Original article: https://reliablecontext.com/articles/gdpr-rectification-erasure-in-append-only-and-event-sourced-systems



In this article

1. The apparent conflict
2. Rectification: correct without erasing the fact it was once wrong
3. Erasure: grounds and exceptions (Article 17)
4. Patterns: tombstone, redaction, payload separation, crypto-shredding
5. Log compaction, snapshots and backups
6. Worked example: Halden Therapeutics AG (fictional)
7. Documenting decisions and Article 30 records
8. Decision table
9. Sources

The apparent conflict

An **append-only log** records new entries without replacing or deleting earlier ones in ordinary operation (glossary). **Event sourcing** stores "the full series of actions taken on an object in an append-only store" and derives current state by replaying it; the event store "is the permanent source of information, so you should never update the event data" (Azure Architecture Center).

The EU General Data Protection Regulation (GDPR) seems to ask for the opposite. Article 5(1)(d) requires that inaccurate data be "erased or rectified without delay"; Article 5(1)(e) limits identifiable storage to "no longer than is necessary"; Articles 16 and 17 give data subjects rights to rectification and erasure. Microsoft's pattern page concedes that an immutable event store "conflicts with data protection regulations that require deletion of personal data".

The conflict is narrower than it looks. Rectification fits an event log, because a correction is itself an event. Erasure is the hard case, and it is mainly a question of where personal data physically lives, so that the history of what happened survives while the identifying payload is destroyed. This article covers EU GDPR. The UK GDPR uses the same article numbers; the UK Information Commissioner's Office (ICO) states that "due to changes made by the Data (Use and Access) Act" its guidance on these rights "is under review" (ICO; Data (Use and Access) Act 2025).

Rectification: correct without erasing the fact it was once wrong

Article 16 gives the right to obtain "without undue delay the rectification of inaccurate personal data", and to have incomplete data completed, including by "a supplementary statement". It does not require destroying the earlier value.

In event sourcing, a correction is a **compensating event**: "a new event that reverses or corrects the effect of a previous event", with the original remaining in the stream (Azure). Whether the superseded value may stay depends on purpose. The ICO's rectification guidance says "it may be possible to argue that the record of the mistake is, in itself, accurate and should be kept", provided the record shows the mistake and the correct information; its example is a medical record that keeps a misdiagnosis alongside the final findings. The EDPB

takes a similar line for ledgers: rectification can sometimes be met by a subsequent transaction cancelling an earlier one, "even though the first transaction will still appear in the chain"; where rectification requires erasure, erasure solutions apply (Guidelines 02/2025, version 2.0, para. 106).

Three design consequences follow:

1. **Every read model shows the corrected value as current.** The history may hold the error; the answer served to a reader may not.
2. **Keep two time axes**, when a fact applied and when it became known, so a correction is not mistaken for a change (reproducing a past state).
3. **Ask whether the wrong value itself must go.** If it has no remaining purpose or is harmful in itself, keeping it may breach storage limitation, and the correction becomes an erasure problem.

Two adjacent duties apply. Under Article 18(1)(a), a data subject contesting accuracy can obtain restriction while the controller verifies; the ICO advises restricting during verification even unasked. Under Article 19, the controller must communicate rectification or erasure "to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort". Article 4(9) defines a recipient as a body to which data are disclosed, "whether a third party or not", so organisations consuming the stream can be recipients; internal copies need the same propagation for accuracy to hold anyway.

Erasure: grounds and exceptions (Article 17)

Article 17(1) requires erasure "without undue delay" where: (a) the data are no longer necessary for their purpose; (b) consent is withdrawn and no other legal ground exists; (c) the data subject objects under Article 21(1) without overriding grounds, or objects to direct marketing under Article 21(2); (d) processing was unlawful; (e) a Union or Member State legal obligation requires erasure; or (f) the data were collected for information society services offered to a child.

Article 17(3) disapplies the right "to the extent that processing is necessary" for freedom of expression; a legal obligation or public-interest task; public health; archiving, research or statistics under Article 89(1); or "the establishment, exercise or defence of legal claims". "To the extent that" is the operative phrase for design: an exception usually covers specific fields for a specific purpose, not a whole record. Erasure in an event store is therefore typically partial. Under Article 12(3), the controller must report action taken within one month, extendable by two months for complex or numerous requests.

The EDPB's 2025 Coordinated Enforcement Action report (adopted 10 February 2026; 32 supervisory authorities, 764 controllers) found seven recurring issues, among them undocumented procedures, misuse of the exceptions, unclear retention periods, deletion in back-ups and ineffective anonymisation. Each has an event-store counterpart.

Patterns: tombstone, redaction, payload separation, crypto-shredding

Four patterns recur. They are layers rather than alternatives, and each leaves something behind.

Pattern	What happens	What remains	Main limitation
Tombstone or erasure event	A new event marks the subject erased; projections drop it	Earlier events and their payloads	Erases nothing from the store by itself
Redaction (rewrite)	Historical events rewritten with personal fields removed	Envelopes and redaction markers	Breaks immutability
Payload separation	Events carry an opaque ID; personal data lives in a mutable store	Events pointing at an ID that no longer resolves	Needs schema discipline from day one
Crypto-shredding	Personal fields encrypted per subject; the key is deleted	Ciphertext and event structure	Legal status of keyless ciphertext is unsettled

Redaction. Azure calls in-place rewriting "a last resort because it undermines the audit trail". The cost is contained by appending a redaction event recording which events changed, when and under which request, without restating erased values.

Payload separation. Microsoft describes storing personal data outside the event store and referencing it by identifier, so "deletion can occur independently without affecting the eventstream". The EDPB recommends the equivalent for ledgers: keep personal data off-chain and put on-chain only a pointer, commitment or keyed hash (paras. 54, 104). It adds that where the strong integrity of a blockchain is not needed, controllers should consider other tools (para. 103). An internal event store is such a tool: its operator can change it.

Crypto-shredding. Where personal data cannot be separated, Microsoft suggests encrypting it "by using a per-subject key" and deleting the key "to render the data unrecoverable while leaving the event structure intact". This is an engineering pattern, not a regulator-endorsed erasure method. The EDPB says key deletion leaves data "unintelligible, at least until the algorithm is broken", and recalls "that encrypted personal data is still personal data" (para. 51). It treats hashes of personal data as personal data too (para. 52).

The counter-argument rests on identifiability. Recital 26 asks what means are "reasonably likely to be used". In EDPS v SRB (C-413/23 P, 4 September 2025), decided under Regulation 2018/1725 (the EU institutions' data protection rules), the Court held that pseudonymised data remain personal for a controller holding the additional information (para. 76), but may not be for a recipient unable to lift the measures or re-identify by other means (para. 77). The inference for crypto-shredding is that once nobody holds the key, nobody can attribute the ciphertext. No source read here confirms that key deletion equals erasure. The EDPB's anonymisation guidelines, which take SRB into account, are in public consultation until 30 October 2026 (EDPB, 8 July 2026). The prudent design uses payload separation with real deletion as the primary mechanism and crypto-shredding for copies that cannot be rewritten.

One constraint covers every pattern: "technical impossibility cannot be invoked to justify non-compliance with GDPR requirements" (EDPB Guidelines 02/2025, para. 50). An event store chosen without an erasure path is an Article 25 design problem, not a defence.

Log compaction, snapshots and backups

Every copy in an event pipeline needs its own erasure path.

Log compaction. Kafka compaction "will always retain at least the last known value for each message key"; a record with a key and a null payload is a tombstone that removes earlier records for that key and is itself cleaned out later (Kafka 4.4 documentation). Three details matter. The active segment is never compacted, so removal is delayed, bounded by `max.compaction.lag.ms`. A consumer lagging more than `delete.retention.ms` (default 24 hours) can miss the tombstone and keep a stale copy. The key survives in the tombstone, so keys should be opaque subject IDs, never email addresses. Microsoft adds that a broker like Kafka "isn't a substitute for an event store".

Snapshots and projections hold decrypted, joined personal data. After erasure they must be deleted or regenerated from the already-redacted stream.

Backups. The ICO says that where a valid request applies, "you will have to take steps to ensure erasure from backup systems as well as live systems", and that "the key issue is to put the backup data 'beyond use', even if it cannot be immediately overwritten" (ICO). In the EDPB action, half of the responding authorities raised back-up concerns, and where modifying back-ups is inadvisable the report expects procedures to "keep track of erasure requests and comply with them on restored systems" (CEF report, Issue 6). For an event store, that means an erasure ledger kept outside the back-up set and replayed after every restore. Crypto-shredding helps only if the key store's own back-ups rotate on a shorter, documented schedule.

Worked example: Halden Therapeutics AG (fictional)

Halden Therapeutics AG, a fictional company, keeps an event-sourced contact store for healthcare professionals at its scientific events. Dr Lena Brandt (fictional) has stream `contact-7f3a`. Name, email and institution live in a separate vault keyed by subject ID; free-text notes in events are encrypted with a per-subject key; deduplication uses a keyed hash of the email under one organisation-wide key.

Rectification. Dr Brandt reports a wrong institution. Halden updates the vault and appends `ContactCorrected {field: institution, basis: Art. 16 request, corrects: event 2}`. Projections refresh, and the external mailing platform that received the old value is notified under Article 19.

Erasure. Later she withdraws consent and objects to direct marketing (Article 17(1)(b) and (c)). One medical-information enquiry falls under a retention obligation Halden's lawyers have documented (a fictional assumption; a real basis needs its own analysis). Everything else goes.

Artefact	After erasure	Still personal data?	Reasoning
Vault entry and its version history	Deleted	No longer held	Primary erasure
Per-subject key	Destroyed	n/a	Crypto-shredding
Encrypted notes in events	Ciphertext remains	Contested; residual risk	EDPB: encrypted data is personal data
Keyed email hash	Deleted	Yes, while present	Shared key keeps it linkable
Event envelopes (type, time, `contact-7f3a`)	Retained	Low risk once vault mapping is gone	Recital 26; SRB

Artefact	After erasure	Still personal data?	Reasoning
Kafka tombstone `contact-7f3a`	Cleaned after `delete.retention.ms`	Opaque key	Propagates the delete
Snapshots, projections	Regenerated from redacted stream	No	Derived copies
Medical-information enquiry	Restricted store, own end date	Yes	Article 17(3)(b), documented
`ErasureCompleted` event	Retained	No contact data	Evidence under Article 5(2)
Back-ups	Beyond use; ledger replayed on restore	Yes, until overwritten	ICO; CEF Issue 6

The row most designs miss is the deduplication hash. Under a shared key, anyone with the key and the email can confirm the subject's presence, and the key cannot be deleted for one person, so the hash itself must go.

Documenting decisions and Article 30 records

Article 5(2) requires the controller to be "able to demonstrate" compliance. For a partial erasure, that means a per-request record: date received, identity checks, grounds, each exception and the data it covers, systems and recipients touched, completion date, and residue with reasons. The EDPB recommends that controllers "verify that erasure has been carried out and be able to demonstrate such erasure" (CEF report). In an event store, that record is another event carrying no erased values.

Article 30(1) requires records of processing that include, "where possible, the envisaged time limits for erasure of the different categories of data" (point (f)) and a description of Article 32(1) security measures (point (g)), which list "the pseudonymisation and encryption of personal data". Article 30(5) exempts organisations under 250 employees unless the processing is likely to result in a risk, is not occasional, or covers special-category or criminal-offence data. The CEF report asks controllers documenting retention periods to "clearly specify any applicable legal obligations". A retention schedule naming each copy (events, vault, snapshots, topics, back-ups, key store) is the operational form of that entry.

Article 25 places the decision "at the time of the determination of the means for processing". The EDPB's Guidelines 4/2019 (version 2.0, 20 October 2020) list storage-limitation elements that read like an event-store checklist: deletion procedures, testing that deleted data cannot be recovered, automation, and "Controllers shall determine what personal data and length of storage is necessary for back-ups and logs" (para. 82).

Decision table

Situation	Approach	Leaves	Document
Error whose history has a purpose	Compensating event; read models show the correction	Superseded value, marked	Purpose for keeping it

Situation	Approach	Leaves	Document
Error with no purpose, or harmful	Correct, then erase the old payload	Correction event only	Erasure record
New system	Payload separation by opaque ID	Envelopes, IDs	Mapping deletion procedure
Existing events with embedded personal data	Redaction with a redaction event; crypto-shredding for new writes	Markers or ciphertext	Residual-risk assessment
Copies that cannot be rewritten	Crypto-shredding, "beyond use", ledger replay on restore	Ciphertext until rotation	Back-up and key-store schedules
Compacted topics	Tombstones on opaque keys; bounded lag	Tombstone, briefly	Consumer-lag monitoring
Part covered by Article 17(3)	Partial erasure; restrict the remainder	Excepted data with end date	Exception and legal basis

This article is educational and describes EU GDPR, with notes on UK practice; it is not legal or regulatory advice.

Sources

1. Regulation (EU) 2016/679 (GDPR), OJ L 119, 4 May 2016 — Articles 5, 12, 16-19, 21, 25, 30, 32; Recital 26.
2. Right to erasure, ICO UK GDPR guidance — back-ups, "beyond use", review notice.
3. Right to rectification, ICO UK GDPR guidance — records of mistakes; restriction during verification.
4. Data (Use and Access) Act 2025, legislation.gov.uk — the Act behind the ICO review notice.
5. EDPB, 2025 Coordinated Enforcement Action on the right to erasure, adopted 10 February 2026 — scope, seven issues, back-up findings, recommendations.
6. EDPB Guidelines 02/2025 on blockchain technologies, v2.0, 7 July 2026 — technical impossibility, encryption, hashing, off-chain storage, erasure and rectification.
7. EDPB Guidelines 4/2019 on Article 25, v2.0, 20 October 2020 — storage-limitation design elements.
8. EDPB news, 8 July 2026 — anonymisation guidelines in consultation until 30 October 2026.
9. CJEU, C-413/23 P, EDPS v SRB, 4 September 2025, ECLI:EU:C:2025:645 — pseudonymised data for controller and recipient (paras. 75-82).
10. Event Sourcing pattern, Microsoft Azure Architecture Center — compensating events, snapshots, payload separation, crypto-shredding.
11. Apache Kafka 4.4 documentation, Log Compaction — compaction guarantee, tombstones, `delete.retention.ms`.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://learn.microsoft.com/en-us/azure/architecture/patterns/event-sourcing

2. https://eur-lex.europa.eu/eli/reg/2016/679/oj
3. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure
4. https://www.legislation.gov.uk/ukpga/2025/18/contents
5. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-rectification
6. https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202502_blockchain_v2_en.pdf
7. https://www.edpb.europa.eu/system/files/2026-02/edpb_cef-report_2025_right-to-erasure_en.pdf
8. https://eur-lex.europa.eu/legal-content/EN/TXT?uri=CELEX:62023CJ0413
9. https://www.edpb.europa.eu/news/edpb-sheds-light-on-anonymisation-and-web-scraping-for-generative-ai-and-adopts-final-version_en
10. https://kafka.apache.org/44/design/design
11. https://www.edpb.europa.eu/system/files/documents/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

THE PUBLISHER

About Reliable Context

Reliable Context is a system of record for organizations that fuse private and public information and must defend every value they act on.

The guarantees

One canonical record per real thing: duplicates resolve by rule, ambiguity is shown rather than hidden, and related organizations relate without ever being merged. A verbatim, cited source and an observation date sit behind every value. Unknowns are declared as not found, blocked or not applicable with a reason, never left as an empty cell. Any past state of the record is reproducible, together with what changed since.

Where it runs

It runs inside the customer's perimeter, one database per organization. Permitted sources, model routing, reader clearance and retention are set as the customer's own policies, and every value is exportable with its chain of custody for an auditor or regulator.

What it is not

It is not a vector database or a RAG framework, not a data catalog, MDM or data-quality suite, not a CRM or data-enrichment vendor, and not a chatbot or AI assistant. Where a reader needs one of those, the honest answer is to say so and point them there.

Visit

See Reliable Context.

Reliable Context is in production use in two sectors; more than six thousand of its identity decisions were made by rule and none has been reversed. Articles published here explain general practice, cite their primary and academic sources, and name the jurisdiction of any regulatory rule they describe. They are not legal, regulatory or compliance advice for a specific organization, and requirements change.

Website: https://reliablecontext.com

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.