GDPR ART. 28(3)(G) · DATA ACT CH. VI

Retention and reversibility commitment

How long REVIEWIT keeps its customers' data, how it erases it, and how a customer leaves the solution with its data and then obtains the certificate of its deletion.

VERSION
1.0 · November 2026

SCOPE
REVIEWIT SAS · REVIEWIT SaaS solution, all regions

DISTRIBUTION
Public

Document issued in French and English; the French version is authoritative.

CONTENTS

01 Roles and retention profiles
02 Retention periods
03 Erasure at expiry
04 Customer exit and return of data
05 Return package
06 Deletion certificate

PURPOSE

Summary of the commitments of REVIEWIT SAS on retention, erasure and return of its customers' data. The authoritative text is the data processing agreement (DPA) version 1.2: its Article 9, the “Retention and reversibility” clause version 1.2 (Annex 3) and Annex 6 “Switching, portability and exit”, which specifies the clause for the Customer's exit and prevails over it on that point.

SECTION 01

Roles and retention profiles

- The Customer is the controller of the data it imports or has imported into REVIEWIT; REVIEWIT acts as processor and applies the periods of the retention profile chosen by the Customer.
- REVIEWIT is the controller of the data specific to the operation and security of the platform (security logs, technical telemetry, internal accounts, contractual and accounting data). Their periods cannot be configured by the Customer.
- No unlimited retention is offered: the contractual ceiling is ten years, unless a higher legal obligation is established and recorded as a reasoned, approved derogation with a review date.
- Any period longer than the Standard profile is recorded with its reason, reference, approver and review date.

PROFILE	EVIDENCE AND BUSINESS AUDIT	SECURITY AUDIT	SOURCE DATA	CAMPAIGN SNAPSHOTS
Standard default	3 years	12 months	Term of the contract	At least 3 years
Regulated	5 years by default, 7 years on request	12 months, extendable with justification	Term of the contract	Aligned with evidence, at least
Custom	1 to 10 years	6 to 36 months	Term of the contract	Aligned with evidence, at least

An “at least” period is a minimum: the data is kept as long as an unpurged certification evidence depends on it, never beyond the ten-year ceiling.

SECTION 02

Retention periods (Standard profile)

CATEGORY	PERIOD	TRIGGER
Temporary collection data	30 days	End of import processing
Live source data	Term of the contract	Termination
Campaign snapshots	At least 3 years, and as long as a certification evidence depends on them	Campaign closure
Certification results	3 years	Campaign closure
Business audit trail	3 years	Recording
Security audit trail	Rolling 12 months	Recording
Technical application log	90 days	Emission
Notification content	90 days	Sending
Proof of sending	1 year	Sending

Generated exports	30 days	Generation
User accounts and profiles	90 days after deactivation	Deactivation
Account configuration	Term of the contract + 90 days	Termination
Non-conformity findings and corrective actions	At least 3 years after closure; an active non-conformity is not purged	Closure of the non-conformity
Hashes of questions asked to the assistant	12 months	Recording
Backups	Rolling 35 days	Creation
Contractual and accounting data	10 years	Close of the financial year
Anonymised statistics	No limit	After irreversible anonymisation

Source: Appendix A of the “Retention and reversibility” clause v1.2 (Annex 3 of the DPA).

SECTION 03 Erasure at expiry

- When its period expires, data is deleted from active systems: databases, interfaces, programming interfaces, exports, search indexes, caches and processing queues. Purging is performed by the product.
- Backups are not modified individually: they expire on a rolling 35-day cycle. Complete erasure therefore occurs no later than 35 days after expiry. REVIEWIT does not commit to any instant deletion.
- Any restoration of a backup reapplies, before the service resumes, the deletions already recorded.
- The chained and sealed audit trail is purged by closed and sealed monthly segments, never record by record; each segment deletion leaves a sealed marker showing that it results from a retention rule and not from tampering.
- A retention measure (hold) that is reasoned, dated, time-limited and reviewed at least once a year excludes the data it covers from purging; placing and lifting it are logged.
- The Customer remains the point of contact for data subjects; REVIEWIT provides the means to search, export and erase a person's data in a subscription, under the reference of the request.

SECTION 04

Customer exit and return of data

Exit applies whatever the reason for the end of the contract. The Customer notifies it in writing and chooses one of three options: switch to another provider, switch to on-premises infrastructure, or have its data erased without return.

STEP	WHEN	WHAT HAPPENS
Exit notice	Receipt	REVIEWIT acknowledges receipt and confirms the timetable: transition, D, extraction period, erasure date.
Notice period	Two months at most	The transition period starts on the date chosen by the Customer, no later than two months after the notice.
Transition	Thirty days at most	The Service continues to be provided; REVIEWIT assists the Customer and the destination provider. The Customer may request an interim package and extend the transition once.
D · end of contract	End of transition	Access to the Service ends. REVIEWIT produces the export, verifies it by an actual restoration, builds the final return package, then deletes the subscription's databases from active systems. Export and deletion are approved by two separate operators and logged.
Making available	No later than two business days after D	The package is delivered through a signed, short-lived download link to the recipient designated by the Customer; the link is renewed on request.
Extraction period	At least thirty days	The package and the export archive remain encrypted in the Customer's region, with no other processing.
Archive erasure	End of the extraction period	The export archive and the package are erased, unless the Customer gives written instructions to keep them.
Complete erasure	No later than D + 65 days	Backups have expired on their 35-day cycle (with extended retention: no later than 35 days after the archive is erased).

- **Erasure without return.** If the Customer chooses erasure, there is no transition period: no package is delivered and the export archive is erased at the end of the contract, no later than thirty days after D.
- **Extended retention.** Before the end of the extraction period, the Customer may ask for the archive and the package to be kept for a period it sets, up to ten years, free of charge. The instruction is recorded with its reason, duration, approver and review date; the Customer may end it at any time.
- **No switching charges.** REVIEWIT imposes no switching or data egress charges, whatever the date of exit. Standard service fees due for the transition period are not switching charges.

SECTION 05

Return package

The package is a ZIP archive of CSV files (UTF-8, semicolon separator, RFC 4180) and JSON files (UTF-8), structured, commonly used and machine-readable formats. Sections and columns carry stable, documented identifiers; no internal name appears.

- Collected directory: identities, accounts, groups, memberships, resources and permissions, collection coverage

- Subscription accounts: roles, assignments, preferences, acceptance of the terms of use
- Campaigns and reviews: frozen scopes, review items, decisions and reasons, assignments, challenges, findings
- Delegations and exceptions; review evidence and attestations, campaign closures, issued reports
- Administrative actions; saved prompts of the RITA assistant; notifications sent
- Audit trail with its sequence, chained hashes and seals, truncated network address
- Subscription configuration: workspaces, connected solutions and connectors (without their secrets), collection scopes, campaign templates, certification rules, retention profile, RITA settings, SIEM destinations, custom e-mail templates
- Documentation in French and English, and a manifest giving the SHA-256 hash and line count of each file, to verify the package's integrity

Excluded: the internal structure of the Service's databases and the technical export archive; REVIEWIT's code and standard catalogues; connector authentication secrets and private keys, never exported (the Customer keeps its own); data for which REVIEWIT is the controller; conversations with RITA, which REVIEWIT does not retain. The exhaustive list is in Article 6 of Annex 6 of the DPA.

SECTION 06 Deletion certificate

- REVIEWIT delivers to the Customer a deletion certificate generated by the platform from its registers, and kept outside the backup cycle.
- An interim certificate is delivered after the export archive is erased; a complete certificate, after the backups have expired.
- It describes the erased scope and lists the retained data with, for each item, its legal basis, the usage restriction applied and its next due date. It records when the return package was made available and the hash of the package delivered.
- After complete erasure, only the data the clause allows to be kept remains: data under an enforceable retention, data for which REVIEWIT is the controller, the deletion register (which holds no identifier of any purged object) and the certificate itself.
- The document “Deletion certificate template” presents its sections.

REVIEWIT SAS · Data protection officer: dpo@we-reviewit.com · Security: security@we-reviewit.com.
Authoritative text: DPA v1.2, Article 9, Annexes 3 and 6.