CONTINUITY · SUMMARY

Backup and recovery strategy

What REVIEWIT backs up, where and for how long, how a restore is carried out, and the recovery objectives REVIEWIT commits to, with their limits.

VERSION
1.2 · November 2026

SCOPE
REVYCORE SAS · REVIEWIT SaaS solution, all regions

DISTRIBUTION
Public

CONTENTS

01 What is backed up
02 Protection and residency
03 Restore
04 Recovery objectives
05 Backups and erasure

PURPOSE

Public summary of REVIEWIT's backup policy. The binding commitments are those of the data processing agreement (DPA): Article 11 and Annexes 5 and 6.

Daily
automatic database backup, point-in-time restore

35 days
retention of database backups in production

24 h
recovery point objective (RPO) committed for a critical or important function

48 h
recovery time objective (RTO) committed for a critical or important function

SECTION 01 What is backed up

ITEM	BACKUP	RETENTION
Databases	Automatic daily backup and restore to a chosen point in time within the retention window; database spread over two availability zones.	35 days in production
Secrets and signing vault (SEAL)	Daily backup, encrypted with the vault's key: without it, a backup cannot be unsealed.	35 days

Export archive of a subscription	Export of the subscription's databases, verified by an actual restore, kept encrypted in the region.	Until its approved erasure
Deletion register	Dedicated storage, outside the backup cycle, append only: it records purges so they can be reapplied after a restore. It contains no personal data.	10 years
Code and infrastructure	Repository of the code and of the infrastructure described as code, kept outside the hosting provider; any release can be rebuilt from its source code.	Full history

SECTION 02 Protection and residency

- Backups are encrypted like the data they protect. The vault and archive keys are deleted only together with the data they protect, since a backup cannot be read without its key.
- Backups are kept in the hosting region chosen by the customer. No copy is made in another region, except on the customer's written instruction: with the "Standard + DR" option, REVIEWIT keeps a copy of the backups in a second region of the same geography.
- Export archives are not publicly accessible.
- Each daily backup is copied to a vault locked in compliance mode, in an account separate from the environment's, in the same region: no administrator can erase it before its term. Backup, copy and restore failures raise an alert.

SECTION 03 Restore

- A restore always targets a new instance: the original instance is never overwritten, and a test never restores into production.
- Under the restore procedure, purges that occurred since the restored point in time are reapplied from the deletion register, erasures on request included; the audit trail chain and database access rights are checked before the service is resumed.
- Switching over to the restored instance is decided by REVIEWIT's management and recorded in the incident register.
- The export of a subscription is verified by an actual restore.
- Each database is restored to an isolated temporary instance, checked read-only, then the instance is deleted; a report measures the recovery time and the data loss. First drills on every database in November 2026: restored in under 30 minutes, with under 10 minutes of data loss. A database with no successful drill in the last 92 days is flagged.
- The restore of the secrets vault and the yearly test of the continuity plan are scheduled.

SECTION 04 Recovery objectives

INDICATOR	COMMITMENT	SCOPE
Recovery point objective (RPO)	24 hours	Service designated by the customer as supporting a critical or important function within the meaning of DORA (Annex 5 of the DPA, section B2)
Recovery time objective (RTO)	48 hours	Same
Monthly availability	99.5%, measured by the public status page (external probes), excluding announced scheduled maintenance	Same

- Lasting loss of the hosting region is excluded from the quantified RPO and RTO commitments; it falls under the business continuity and recovery plan (Annex 5 of the DPA, Article 22). The copy in a second region, on the customer's written instruction, is described in section 02.

SECTION 05 Backups and erasure

- Backups are not modified individually: they expire on their rolling thirty-five-day cycle.
- At the end of the contract, complete erasure of the customer's data, backups included, is achieved no later than sixty-five days after the end of the contract; where retention is extended on the customer's instruction, no later than thirty-five days after the export archive is erased.
- The export archive and the return package are kept encrypted in the customer's region during the extraction period, then erased; a certificate of deletion is given to the customer.

REVYCORE SAS · Security: security@we-reviewit.com · Data protection: dpo@we-reviewit.com. Reviewed annually and after any major change to the backup policy. The French version is authoritative.