SYMBEEO

PUBLIC

DESIGN STUDY

Tested exit and 15-minute recovery point for a drug maker's GxP records on Azure

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Cloud	Life Sciences	EU drug maker
DOCUMENT	**VERSION**	**DATE**
CLD-006	1.1	Oct 10, 2026

WRITTEN BY

Steve Phillips, Principal Data Center Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	CLD-006	Version	1.1
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Sep 27, 2026
Capability	Cloud	Industry	Life Sciences
Author	Steve Phillips	Role	Principal Data Center Architect
Credentials	CCSP, CCIE, AWS Certified Security – Specialty		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 8
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure read from the vendor's or publisher's own current page on Sep 24, 2026, or on Sep 27, 2026 where marked · [S*] figure from a secondary publisher where the provider's own page was not read · [A] design assumption, to be confirmed by the signing engineer · [T] design target: the record's outcome figure and anything derived from it. No figure comes from any engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Sep 27, 2026	1.0	First issue.
Oct 10, 2026	1.1	Approval line now reads: approved by the Founder, issued by Symbeeo. Steve Phillips remains the author.

1 · Scope

Who it is for. The head of IT quality at a pharmaceutical manufacturer whose quality-management and laboratory systems run on Azure, and whose inspectors and board ask two questions the company cannot yet answer with evidence: can the records survive the loss of a region inside four hours, and can the company actually leave this provider if it must?

Typical buyer [A]. An EU drug maker with two manufacturing sites. Two tier-1 GxP workloads on Azure: a quality-management system and a laboratory information system. Each runs on VMs with an Azure Database for PostgreSQL flexible server (0.8 TB and 1.2 TB) and keeps its record files in Blob Storage, 60 TB in total, under time-based retention. Longest retention class: 15 years. A private-cloud pod (SRA-DC-001) runs in the company's own data center.

What is in. Tier-1 recovery to a second Azure region, record immutability through failover, the yearly exit test of one workload to the private-cloud pod, the export formats, the switching timetable and cost position, and the validation evidence QA signs. This is SRA-CLD-001 R15, R16, F4 and F8 applied to one estate. **What is out.** The applications' own validation; the landing zone and connectivity (CLD-002 and CLD-003 show the pattern); moving the workloads permanently.

Assumptions. Both Azure regions are in the EU and approved for the data [A]. The application vendors support PostgreSQL 18 on-premises [A]. The pod has an S3-compatible object store with object lock and 80 TB free [A]. QA accepts a validation protocol per test as the record [A].

Related documents, read Sep 24, 2026.

- Microsoft, business continuity in Azure Database for PostgreSQL flexible server — https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/concepts-business-continuity
- Microsoft, supported versions of PostgreSQL in Azure Database for PostgreSQL — https://learn.microsoft.com/en-us/azure/postgresql/configure-maintain/concepts-supported-versions
- Microsoft, immutable storage for blob data — https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview
- Microsoft, Azure storage disaster recovery planning and failover — https://learn.microsoft.com/en-us/azure/storage/common/storage-disaster-recovery-guidance
- European Commission, Data Act explained — https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

© 2026 Symbeeo. All rights reserved. · Public

- Regulation (EU) 2023/2854 (Data Act), Official Journal text, Art. 2(35)–(36), 25(2)(a), 29, 34 and 50, read Sep 27, 2026 from the Publications Office — http://publications.europa.eu/resource/celex/32023R2854
- Garrigues, Data Act and cloud switching (secondary source for the 30-day transitional period) — https://www.garrigues.com/en_GB/garrigues-digital/data-act-and-cloud-switching-keys-new-rules-changing-cloud-service-providers
- UK CMA, cloud services market investigation, Appendix N (egress fees and free switching) — https://assets.publishing.service.gov.uk/media/688b8169fc784fa12a089071/Appendix_N_-_Egress_fees___free_switching_programmes.pdf

1c · Public implementations this design follows

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
PostgreSQL flexible server recovery table: geo-restore RPO under 1 h; cross-region read replica RPO "typically ranging from 30 secs to 5 Minutes"; zone-redundant HA RTO under 120 s, RPO 0	Microsoft Learn · updated Sep 15, 2026 · vendor documentation, used to build our own design	R4, R5 and §4.1: replica, not geo-restore, for a 15-minute RPO	https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/concepts-business-continuity
Immutable blob storage: locked time-based retention cannot be deleted or shortened; assessed by Cohasset against SEC 17a-4(f), FINRA 4511 and CFTC 1.31; policy changes after the last sync do not reach the secondary on failover	Microsoft Learn · updated Aug 18, 2026 · vendor documentation, used to build our own design	R6, R7 and §4.2	https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview
Provider free-switching programs reviewed by a regulator: Microsoft's "is for full switching only and does not apply to partial switches for workloads or a single service"	UK CMA, final decision appendix · Jul 31, 2025 · published standard, used to build our own design	R12 and §4.5: the provider's free-exit program does not cover a one-workload exit test	https://assets.publishing.service.gov.uk/media/688b8169fc784fa12a089071/Appendix_N_-_Egress_fees___free_switching_programmes.pdf

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Tier-1 estate	2 workloads · PostgreSQL 0.8 TB and 1.2 TB · 60 TB of record files	[A]
R2	Recovery point	≤ 15 min of data after loss of the primary region	[T]
R3	Recovery time	≤ 4 h to running in the second region	[T]
R4	Database replication	cross-region read replica, typical RPO 30 s to 5 min	[S] PostgreSQL business continuity table

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R5	In-region failure	zone-redundant HA: RTO under 120 s, RPO 0	[S]
R6	Record immutability	record containers under locked time-based retention: cannot be deleted, only extended	[S] immutable storage
R7	Retention length	15 years for the longest class, inside the 146,000-day maximum	[A]; [S] maximum
R8	Exit test	one tier-1 workload exported and running at the target place ≤ 30 days, every 12 months	[T]
R9	Export formats	databases as PostgreSQL dumps plus CSV per table; files as stored, with a SHA-256 and retention-date manifest	[T]
R10	Target place	private-cloud pod: PostgreSQL 18 on VMs, S3-compatible object store with object lock	[A]
R11	Switching charges	no switching charges, egress included, for a switching process from January 12, 2027 (Art. 29(1)); in parallel use, egress may still be charged at cost (Art. 34(2))	[S] Regulation (EU) 2023/2854, read Sep 27, 2026
R12	Provider free-exit program	applies to a full exit only, not to one workload	[S*] UK CMA
R13	Evidence	every recovery and exit test recorded in a validation protocol signed by QA	[T]
R14	Version parity	same PostgreSQL major at source and target: 18 (18.6 current on Azure)	[S] supported versions

Fourteen rows; seven carry a published figure, two are design assumptions, five are design targets.

3 · Architecture overview

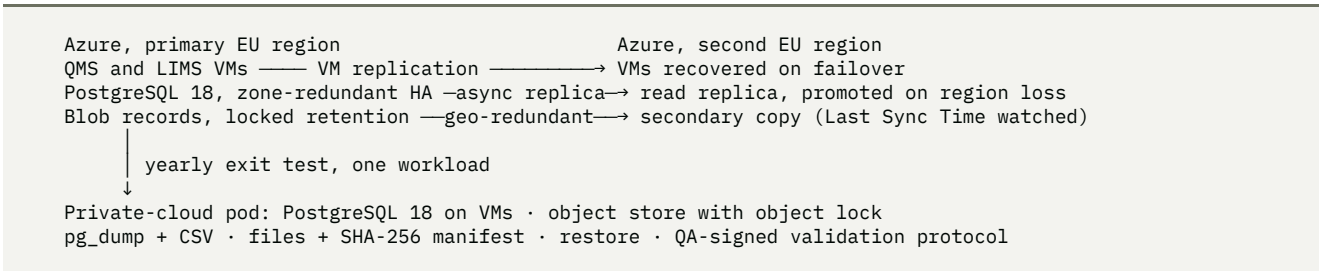


Figure 1. Region failover and yearly exit test

Two tests the inspectors can read: a region failover that shows the records back within four hours and fifteen minutes of data, and a yearly exit that shows one whole workload running outside Azure within thirty days from files in open formats.

© 2026 Symbeeo. All rights reserved. · Public

Table 4. Architecture overview

Role	Product (exact model)	Qty	Capacity used	Why this unit
Database	Azure Database for PostgreSQL flexible server, PostgreSQL 18	2 servers + 2 replicas	0.8 and 1.2 TB [A]	18.6 current [S]; replica RPO 30 s–5 min [S]
Record store	Azure Blob Storage, GRS, locked time-based retention	1 account per workload	60 TB [A]	WORM, Cohasset-assessed [S]
VM recovery	Azure Site Recovery	1 vault in the second region	application VMs [A]	named by Microsoft for regional VM protection [S]
Exit copy tool	AzCopy and pg_dump	1 each	the tested workload's share of the 60 TB and 2 TB [A]	AzCopy named by Microsoft for copying out [S]; pg_dump named for table export [S]
Exit target	private-cloud pod (SRA-DC-001)	1	one workload at a time [T]	the company's own place [A]

4 · Design by subsystem

4.1 Databases.

PostgreSQL 18, the newest major Azure offers, 18.6 at the time of reading [S]. Zone-redundant HA in the primary region: RTO under 120 seconds, RPO zero [S] (R5). A cross-region read replica in the second region: replication is asynchronous and "might lag the primary", with RPO typically 30 seconds to 5 minutes [S], inside R2. On region loss the replica is promoted to a standalone server [S]. Rejected: geo-restore from geo-redundant backups — RPO under one hour and RTO that varies with size [S]; it fails R2.

4.2 Records.

Each record container carries a time-based retention policy, locked within 24 hours of testing, as Microsoft recommends [S]. A locked policy cannot be deleted and its period can only be extended [S]; the longest class is 15 years [A], well inside the 146,000-day maximum [S]. The accounts are geo-redundant; immutability works with customer-managed failover, but a policy change made after the last sync does not reach the secondary [S], so every policy change is followed by a check that Last Sync Time has passed it [A]. Last Sync Time lag above 15 minutes raises an alarm (R2) [T]. Rejected: version-level WORM — it needs versioning and blocks the container-level legal holds QA uses for investigations **[S][A]**.

4.3 Region failover.

Order: promote both replicas; fail the storage accounts over (customer-managed unplanned failover, typically under one hour [S]); recover the application VMs with Site Recovery [A]; QA runs the record-integrity check. After an unplanned storage failover the account is locally redundant in the new primary and the original primary copy is deleted [S], so geo-redundancy is re-enabled at once and the replicas re-created [A]. Target: four hours end to end (R3) [T]. Rejected: waiting for a Microsoft-managed failover — Microsoft itself says not to rely on it [S].

4.4 Exit test.

Yearly, one workload in turn [A]. Databases: `pg_dump` in directory format plus a CSV per table [T], restored with `pg_restore` into PostgreSQL 18 on the pod (R14). Files: copied with AzCopy [S] into the pod's object store under object lock with the same retain-until dates, a SHA-256 manifest proving every file arrived unchanged [T]. The application is then started on the pod against the restored copy and QA runs the workload's own acceptance script; the protocol

© 2026 Symbeeo. All rights reserved. · Public

records dates, hashes, row counts and the signature (R13). Thirty days is the budget (R8), matching the Data Act's maximum transitional period of 30 calendar days, Art. 25(2)(a) [S] (read Sep 27, 2026). Rejected: storage account failover as the exit route — Microsoft states failover is not for migration [S].

4.5 Switching cost.

The Data Act has applied since September 12, 2025 (Art. 50). Switching charges include data egress charges (Art. 2(36)); until January 12, 2027 a provider may charge reduced switching charges up to its costs, and from that date none for the switching process (Art. 29(1)–(3)) [S]. Where a service is used in parallel with another, the provider "may impose data egress charges, but only for the purpose of passing on egress costs incurred" (Art. 34(2)) [S] (all read Sep 27, 2026). The yearly test copies one workload out while it keeps running on Azure, which reads as in-parallel use, not a switch; whether a given test counts as switching is the client's legal question [A]. Microsoft's free-exit program covers a full exit only [S*]. The design therefore budgets egress at cost for every test, before and after January 2027: the tested workload's share of the 62 TB estate (60 TB of files and 2 TB of databases, R1), set by the week-1 inventory [A]. Rejected: moving the test to February 2027 to avoid the charge — Art. 34(2) can still apply.

4.6 Evidence.

One validation protocol per failover test and per exit test: plan, pass criteria (R2, R3, R8), results, deviations and QA signature (R13) [T]. The protocols are the evidence behind the company's exit plan when an inspector or the board asks for it [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
One availability zone lost	database fails over to the standby in under 120 s with no data loss	[S] zone-redundant HA
Primary region lost	replicas promoted, storage failed over, VMs recovered; ≤ 15 min of data lost, running ≤ 4 h	[S] replica RPO; [T] R2, R3
Replica lag above 15 min at the moment of loss	recovery point misses R2; the gap is recorded as a deviation	[S] lag possible; [A]
Retention policy changed just before the loss	the secondary keeps the older policy; re-applied after failover	[S] changes after last sync not replicated
Exit restore fails a row-count or hash check	test stops; source untouched; defect raised, re-run within the 30 days	[T] R8, R9
Application will not start on the pod	protocol records a failed exit; the vendor's on-premises support is engaged	[A]

6 · Limits

- The replica's recovery point is "typically" 30 seconds to 5 minutes [S], not a guarantee; heavy write bursts can widen it.
- Storage replication has no stated recovery point on the page read; the design watches Last Sync Time rather than assuming one.

© 2026 Symbeeo. All rights reserved. · Public

- A one-workload exit test pays egress before January 12, 2027 [S][S*] and may still pay it at cost afterwards as in-parallel use, Art. 34(2) [S]; the exact figure depends on the price list on the day and the workload's share of the 62 TB.
- The exit test proves the data leaves in open formats and the application runs; it does not re-validate the application on the pod.
- Database sizes, file volumes and the 15-year class are assumptions; the week-1 inventory sets them.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

8 · The author

WRITTEN BY

Steve Phillips

Principal Data Center Architect

CCSP, CCIE, AWS Certified Security – Specialty

Signed off by Edwin Ozer, Founder.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

CLD-006 · Version 1.1 · Oct 10, 2026