Your Keys. Your Data. Your Choice of Cloud.

A plain-language guide to who holds the password to unlock your data

Rediacc | 2026

Why Regulators Now Care Who Holds Your Keys

From best practice to legal baseline

Encryption used to be a "should." Now it is a "must."

GDPR Article 32 names encryption as a required safeguard. Fines reach 10 million euros or 2% of global revenue (GDPR Article 32).

Meta was fined **91 million euros** in September 2024 for storing passwords in plain text (DPC Ireland 2024).

Total GDPR fines have hit about 5.88 billion euros as of January 2025 (GDPR Enforcement Tracker 2025).

GDPR also offers a reward. If breached data was encrypted, you may not need to notify each person (Article 34(3)(a)).

In 2020, the EU's top court ruled in a case called **Schrems II**. The ruling: EU data cannot sit on a US server where US courts can grab it.

The trigger was a US law called the **CLOUD Act**. It lets US courts demand data from any US cloud firm, anywhere in the world.

The fix is encryption where **you alone hold the keys**. If the vendor never had your keys, a court order finds nothing.

> Ask your DPO: do we hold our own keys for EU customer data, and would they pass a Schrems II review?

Health Data: The Safe Harbor Math

Why HIPAA makes key control worth real money

If your company touches health data, this matters. If not, the same idea applies to your cyber insurance. Encryption vendors can't unlock means breach rules don't apply.

A HIPAA rule called the safe harbor says this. If stolen health data was encrypted, and the thief did not get the key, it is not a reportable breach.

That means no patient letters, no federal filing, no press release.

The average healthcare breach costs **over 10 million dollars** (IBM 2024). The bill grows once you add notice costs, fines, and lawsuits.

HIPAA fines reach 68,928 dollars per violation. The yearly cap is 2,067,813 dollars (HHS OCR 2024).

Advocate Health Care paid **5.55 million dollars** for breaches (HHS OCR 2016). The cause was laptops that were not encrypted.

Holding your own keys is the gap between a quiet incident and a public crisis.

> Ask your compliance lead: would our backup encryption qualify us for HIPAA safe harbor today?

What Each Major Rule Actually Demands

A quick map for the compliance binder

PCI-DSS 4.0 took effect on April 1, 2025.

It expands encryption rules and bans disk encryption as the only protection for live card systems (PCI SSC 2025).

Fines from card brands run **5,000 to 100,000 dollars per month** until you fix it (PCI SSC 2025).

California's CCPA and CPRA let consumers sue when raw data leaks. Damages run 100 to 750 dollars per person per leak (CCPA §1798.150).

A breach hitting 100,000 customers can mean **10 to 75 million dollars** in payouts.

Rule	Max penalty
GDPR	20M euros or 4% of global revenue
HIPAA	2.07M dollars per year, per type
PCI-DSS 4.0	100K dollars per month
CCPA / CPRA	750 dollars per person per incident

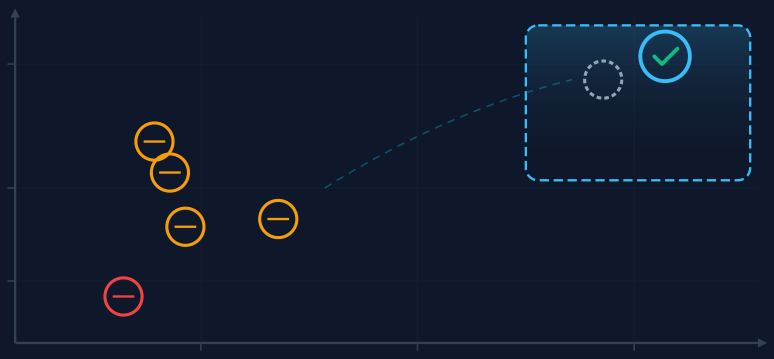
The SEC rule from December 2023 makes public firms report a serious hack within four business days. Fines reach 25 million dollars (SEC 2023).

NIST 800-171 requires strong encryption for federal contractors. Fail it and you can lose contracts, plus face fraud lawsuits.

> No single rule fits all. Customer-held keys with full logs come closest.

The Backup Vendor Encryption Problem

Every vendor either holds your keys or locks your data



Every major backup vendor does one of two things. They hold the keys for you. Or they let you bring your own keys, but lock the data into their format.

Veeam uses a password you set. They store it inside their own database. **Lose the password or the database, you lose your data.**

Rubrik lets you bring your own keys through Amazon, Microsoft, or other key services. But the backup files use a Rubrik-only format called Atlas. Only Rubrik software can read it.

Druva is the most locked in. It runs only as a cloud service, on Amazon, with Amazon keys.

There is no clean way to walk away without a full decrypt-transfer-re-encrypt project.

> Ask your backup vendor: if I cancel tomorrow, can I read my backups using my own tools?

How the Cloud Providers Lock You In

Their keys, their data, their cloud

Commvault stores keys in its own database. Cohesity uses its own file format. Once enabled, it cannot be turned off.

The big three cloud providers set the same trap. Data locked by **Amazon's key service only unlocks with Amazon's key service**.

Microsoft keys only restore to Microsoft. Google keys only work in Google.

Vendor	Can you read backups without them?
Veeam	Only with their software plus your password
Rubrik	No, Atlas format only
Druva	No, Amazon-only
Cohesity	No, own format only

For the big three clouds, Amazon, Microsoft, and Google data only unlocks in that same cloud.

Key services like Thales, HashiCorp, and Fortanix do solve key portability. But they cost **50,000 to 500,000 dollars or more per year** in fees (vendor pricing 2025). That prices out most mid-sized firms.

Think of it like renting a storage unit. In one, you bring your own padlock. In the other, the storage company holds the master key.

If the police ask the company for the key, only in the first case is there nothing to hand over.

What Switching Vendors Actually Costs

90,000 to 300,000 dollars per petabyte, before you re-encrypt

When you switch backup vendors, the old keys cost you three times. You pay to decrypt the data. You pay to move it. You pay to re-lock it with the new vendor.

Moving data out of a cloud costs 8 to 15 cents per gigabyte (AWS pricing 2025). Moving 1 terabyte costs 90 to 300 dollars.

Moving a petabyte costs **90,000 to 300,000 dollars** before any other expense. Apple reportedly pays 50 million dollars a year in these fees to Amazon alone (The Information 2023).

Even at fast speeds, moving a petabyte takes 9 to 10 days of nonstop transfer (10 Gbps math). Moves for firms with 500 or more servers run 3 to 6 months. Complex setups often take 12 months.

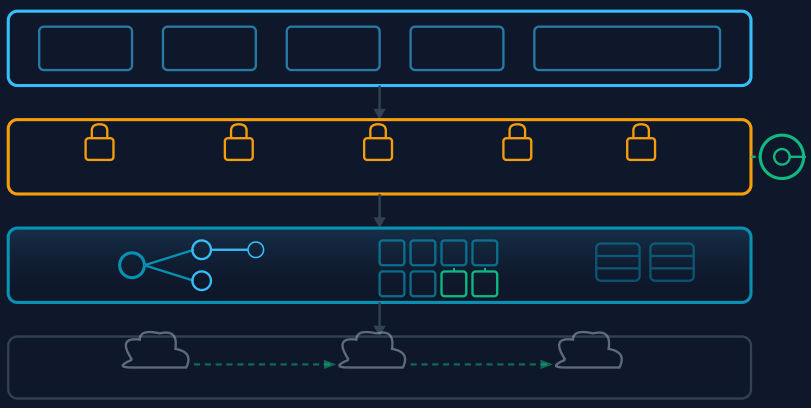
Gartner says downtime can cost over 300,000 dollars an hour (Gartner 2024). A mid-sized firm with 150 million dollars in revenue loses about 17,123 dollars an hour.

Ten days of migration downtime can mean **a 4 million dollar loss**.

> Gartner predicts that by 2027, more than 60% of organizations will move to vendor-neutral key services (Gartner 2024).

How Rediacc Removes the Switching Penalty

Encryption that travels with your data



Rediacc builds on an open storage layer called btrfs. It is free, open source, and built into Linux.

Think of your data as having two locks. One lock is held by the vendor, one by you.

With most backup vendors, both locks turn at the vendor's site. With Rediacc, your lock works anywhere.

The storage layer encrypts every block of data before it touches the disk. Your key, only yours, locks each block.

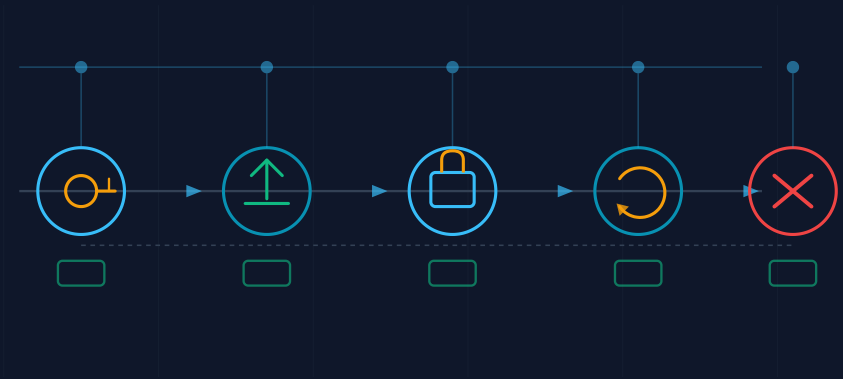
When you move clouds, the encrypted blocks travel as is. No decrypting on the way out, no re-encrypting on the way in.

The same trip that costs **90,000 to 300,000 dollars** in network fees with a regular vendor becomes a straight data transfer. The savings are real because the work simply does not have to happen.

Migration becomes a safe-deposit box you can move from one bank to another, without the bank ever opening it.

You Generate the Key. You Keep It.

Zero-knowledge means the vendor never sees it



A recent Thales study of 3,200 firms across 20 countries found that **57% of organizations use five or more key systems** to manage their data (Thales Data Threat Report 2025). That is up from 53% the year before (Thales Data Threat Report 2025).

48% still manage keys through their cloud provider's console (Thales Data Threat Report 2025), which ties them to that provider forever.

Rediacc works differently. You generate your encryption key on your own systems.

Rediacc never creates it, never stores it, never sees it. The vendor cannot hand over what it does not have.

This is the practical answer to the CLOUD Act and Schrems II risk on slide 2. If your vendor holds your keys, a court order can reach them. If your vendor never had your keys, there is nothing to compel.

> Ask your vendor in writing: can you decrypt our backups if a court orders you to? The right answer is no.

Keys Rotate Without Re-Encrypting Everything

Distribution, rotation, and one audit log

The hardest part of managing keys is rotation.

PCI-DSS 4.0 needs regular rotation and a full record of it (PCI-DSS 4.0 §3.6).

Most firms fall behind. Rotating a key usually means re-encrypting every old backup, which is slow and costly.

Rediacc swaps the key without re-locking each file. Old backups open with the old key; new backups use the new key.

You stay compliant. No multi-week project each time you rotate.

The system writes one audit log that maps to all four rules at once: GDPR Article 32, HIPAA safe harbor, PCI-DSS 4.0, and SOC 2.

For the **57% of firms drowning in five or more key systems** (Thales Data Threat Report 2025), this turns key sprawl into a single dashboard.

> Ask your auditor: would a single log covering GDPR, HIPAA, PCI, and SOC 2 reduce our annual audit hours?

Your Keys. Your Data. Your Choice of Cloud.

Hold your own encryption keys. Move clouds without re-encrypting.

Pass GDPR, HIPAA, PCI-DSS 4.0, and SOC 2 audits from one log.

See how it works at rediacc.com

rediacc.com