eBlocks Software
data driven digital solutions

ONTRACK AI INSIGHTS

Encryption is necessary. But it is not enough.

Four custody models. The difference is who can decrypt.



Provider-managed
Provider can decrypt

Customer-managed
Provider can decrypt

Bring your own key
Provider can decrypt

Hold your own key
Provider cannot decrypt*

GOVERNANCE

EXCLUSION

* Requires an architecture that denies the provider access to keys and plaintext.

eBlocks Software
data driven digital solutions

What follows.

I **The question a review should answer**
And the three it usually answers instead

II **Four custody models**
What each provides, and what it does not

III **Feasibility and trade-off**
Why the practical objection has expired

IV **The South African position**
POPIA, Directive 3, and why this is a compliance question

V **Four questions for a provider**
To ask before the next review closes

The question a review should answer.

It is narrow, and it is testable.

What can they actually produce?.

Sovereignty reviews typically confirm three things: where data is stored, whether it is encrypted at rest and in transit, and who administers the keys.

All three are necessary. None answers the question that determines the outcome.

If the provider receives a lawful order from a foreign authority, what are they technically able to produce?

If the answer is readable data, the sovereignty position rests on the provider's willingness and on contract terms. If it is ciphertext the provider cannot open, the position rests on cryptography, and the request must return to the customer in the customer's own jurisdiction.

> **The difference is decided by key custody,**
> **and by nothing else in the review.**

Encryption protects data from parties without the key.

Asked whether cloud data is encrypted, most organisations answer yes, correctly. Encryption at rest is the default in almost every major service.

It establishes nothing about who holds one.

In the default configuration the provider generates the key, stores it, and performs every cryptographic operation with it.

The data is encrypted and the provider can decrypt it. Both statements are true simultaneously. Only the first is typically reported.

Four custody models.

Three differ in governance. They are identical in exposure.

Three of these are the same.

MODEL	WHAT IT GIVES YOU	PROVIDER CAN DECRYPT
Provider-managed	Operational simplicity. Nothing else.	Yes
Customer-managed	Lifecycle control, revocation, an audit trail.	Yes
Bring your own key	Control of key generation. You are root of trust.	Yes
Hold your own key	The key never enters the provider's environment.	No

An entity that retains the technical ability to use a key can be compelled to use it.

Only the fourth changes what an order produces.

Customer-managed keys provide revocation and evidence. Access can be withdrawn, and there is a record of who did what.

Bring-your-own-key provides control of key generation, establishing the customer rather than the provider as root of trust.

Both are worthwhile. Neither removes the provider's technical capability to decrypt.

The terminology obscures this. “Customer-managed” describes who administers a key, not who possesses it, and the two are indistinguishable in summary reporting.

Under hold-your-own-key the distinction is not contractual or procedural. There is no key in the provider's possession to be compelled to use.

The practical objection has expired.

Hold-your-own-key architectures are supported by the major providers. AWS offers External Key Store, Google Cloud offers External Key Manager, and Microsoft has extended Azure Key Vault Managed HSM in the same direction.

These capabilities were built in response to demand from regulated customers.

The material trade-off is availability. If the customer's key manager is unreachable, the data is unreachable. This is a real dependency and it does not diminish with maturity.

It follows that key custody should be assessed per workload rather than applied uniformly. Applying sovereign custody to every dataset increases cost and operational risk without a corresponding reduction in exposure.

IV

The South African position.

This is a compliance question, not only a security one.

Neither instrument prescribes a custody model.

POPIA restricts cross-border transfers of personal information unless the recipient is subject to protections substantially similar to its own conditions. A provider that can be compelled to decrypt is relevant to that assessment.

For banks, the Prudential Authority's Directive 3 of 2018 requires that cloud computing and the offshoring of data must not inhibit a regulator's ability to fulfil its duties. An arrangement in which a foreign authority can obtain readable data without the institution's knowledge is material to that requirement.

Both make the question relevant to compliance, not merely to security.

Ask them in writing.

01 Where does the key material physically reside, and under whose operational control?

02 Can any cryptographic operation be performed without our key manager being involved?

03 On receipt of a lawful order, are you permitted to notify us?

04 Which legal entity is answering these questions, and under which jurisdiction is it incorporated?

The fourth is frequently the most revealing. The contracting entity is often not the entity named on the invoice, and the answer determines which legal system reaches the arrangement.

eBlocks Software
data driven digital solutions

Necessary, and insufficient.

A sovereignty review that confirms encryption without establishing key custody has verified a control, not an exclusion.

Indistinguishable in summary reporting.
Decisive under legal process.

eBlocks Software
data driven digital solutions

What this is built on.

Protection of Personal Information Act 4 of 2013
Fully enforceable from 1 July 2021. Amended regulations effective April 2025.

Directive 3 of 2018, Prudential Authority, SARB
Cloud computing and offshoring of data. Effective 1 October 2018.

Clarifying Lawful Overseas Use of Data Act
United States, 2018.

AWS External Key Store; Google Cloud External Key Manager
Provider documentation on external key management.

Azure Key Vault Managed HSM
Microsoft documentation on external key management.

General commentary, not legal advice.

eBlocks Software
data driven digital solutions

Bring the document it was built from.

Twenty minutes, in your own board. We will walk it through the loop and show you exactly where the evidence breaks.

eblocks.co.za/ontrack-ai Book a demo →

Deon Thomas · CEO, eBlocks Software
solutions@eblocks.co.za