WHITEPAPER

365CONNECT

CUSTOMER-MANAGED KEYS (CMK) AND WHAT DATA SOVEREIGNTY REALLY MEANS ACROSS THE DYNAMICS365 ESTATE.

WHO HOLDS YOUR KEYS?

DATA SOVEREIGNTY IN DYNAMICS 365.

VERSION	0.1
DATE	1 JUNE 2026
AUTHOR	PATRICK MOUWEN, PRINCIPAL ARCHITECT
PREPARED FOR	D365 COMMUNITY MEMBER
CLASSIFICATION	COMMUNITY BRIEF

IS YOUR DYNAMICS 365 DATA SOVEREIGN?

MOST ORGANISATIONS CONFLATE TWO SEPARATE QUESTIONS

CMK SOLVES THIS

KEY CONTROL

WHO CAN DECRYPT AND READ YOUR DATA?

- YOU SUPPLY YOUR OWN RSA KEY
- REVOKE KEY MICROSOFT LOCKED OUT
- AZURE KEY VAULT + ENTERPRISE POLICY
- ROTATE ON DEMAND, NO DOWNTIME

CMK DOES NOT SOLVE THIS

DATA RESIDENCY

WHERE DOES YOUR DATA PHYSICALLY LIVE?

- GOVERNED BY TENANT HOME GEO
- EU DATA BOUNDARY WHERE APPLICABLE
- MICROSOFT SOVEREIGN CLOUD
- CMK DOES NOT MOVE DATA

“BRING YOUR OWN KEY CONTROLS WHO CAN READ THE DATA - NOT WHERE IT LIVES.

Data Sovereignty & Customer-Managed Keys in Dynamics 365

Context

A D365 Community Member raised a question: customer-managed keys (CMK) can be issued to encrypt data but does that also hold for Dynamics 365?Her instinct was that it works through the Power Platform layer, while clear Microsoft documentation was hard to pin down. This brief confirms that instinct and maps where CMK does, and does not, reach across the Dynamics 365 estate.

TWO MEANINGS OF SOVEREIGNTY

The term “data sovereignty” is used interchangeably for two different things: (1) key control who is able to decrypt the data, which is what CMKaddresses; and (2) data residency where the data physically lives (tenant home geo, EU DataBoundary, Sovereign Cloud). CMK answers the first, not the second. Clarifying which one the businessactually needs avoids talking past each other.

Solution

GENERAL SOLUTION ACROSS THED 365APPS

There is no separate “Dynamics 365 CMK” feature. CMK is the Power Platform customer-managed key capability, applied to the Dataverse environment through an enterprise policy. You supply your own RSA / RSA-HSM key in Azure Key Vault, create a Power Platform enterprise policy that references it, grant that policy access to the vault, and then assign the environment to the policy. Dataverse re-encrypts the environment data with your key. So, the Community member’s instinct is correct: the mechanism runs through the Power Platform layer.

Mapped to the two dimensions of sovereignty:

- Key control CMK lets you rotate or swap the key on demand and, crucially, revoke Microsoft’s access. Once the key is revoked, the data becomes undecipherable to the service. That revocation is the real sovereignty pay-off. Azure Managed HSM (FIPS 140-2 Level 3) strengthens this further.
- Data residency CMK does not move data. Where data sits is governed separately by the tenant’s home geo and, where applicable, the EU Data Boundary / Microsoft Sovereign Cloud. Applying a CMK does not change the location of the data.

> *Bring your own key controls who can read the data not where it lives.*

GENERAL LIMITATIONS(NOT COVERED BY CMK)

CMK is deliberately scoped to data at rest in the environment. The following are not encrypted with your key and remain under the Microsoft-managed key:

- Connector / connection settings and Power Platform environment settings.
- Power Apps display names, descriptions, and connection metadata.
- Pre-existing Power Automate flows present in the environment when CMK is applied these continue to use the Microsoft-managed key.
- Lifecycle Services (LCS) metadata such as file assets, methodologies, and Task Recorder data.
- Some add-ins (e.g. Tax Calculation and Electronic Invoicing via stand-alone RCS) had partial or no CMK support verify against current docs.
- Operational reality: encryption at rest does not stop operator access while data is in use only key revocation locks Microsoft out of data at rest. CMK also requires a Managed Environment with appropriate licensing, and enabling it causes downtime while the environment is encrypted.

Solution per D365 app domain

FINANCE & OPERATIONS (D365 ERP)

For finance and operations apps Finance, Supply Chain Management, Commerce, Project Operations, Intelligent Order Management, and Human Resources CMK is delivered through Power Platform and applies only when Power Platform integration is enabled for that environment. Without integration, F&O continues to use Microsoft-managed keys. Once enabled and assigned to the enterprise policy, CMK also covers the environment-specific resources: the SQL databases and Azure storage accounts. One sequencing caveat: do not enable CMK in a pre-existing Power Platform environment before wiring up the F&O integration.

D365COMMERCE CSU

Commerce inherits the F&O behaviour, but with edges that matter for retail. CMK covers the F&O environment resources except the e-commerce CMS and recommendations. More importantly for channel architecture: CMK cannot be applied to Commerce Scale Units, e-commerce, and ratings & reviews components that sit in a different geo than the F&O environment CMK is enabled for. So “is all my retail/channel data under my own key?” has a nuanced answer confirm CSU geo placement before making a hard statement.

> CSU CAVEAT
> Channel-sidedatain a Commerce Scale Unit located in a different geo from the F&O environment falls outsidetheCMK policy. This is the most common gap in retail sovereignty conversations, and worth flaggingexplicitly before anyone assumes end-to-end coverage.

POWER PLATFORM

This is the home of the feature. Dataverse (custom solutions and Microsoft services), Power Automate, and Copilot for model-driven apps are CMK-encryptable. Azure Key Vault key versioning allows on-demand rotation and key swap with no downtime for Dataverse environments. A subset of surfaces (see general limitations above) remains under the Microsoft-managed key.

D365 APPSCE, FIELD SERVICE, CUSTOMER INSIGHTS

The Dataverse-native business apps Sales, Customer Service, Field Service, Customer Insights – Data, and Chat for Dynamics 365 are covered directly once CMK is applied to the Dataverse environment, because their data lives in Dataverse.

Sources (evidence)

All findings above trace back to first-party Microsoft documentation, cross-checked with current community material:

- Manage your customer-managed encryption key Power Platform (http://learn.microsoft.com/power-platform/admin/customer-managed-key) canonical reference incl. the supported-apps list.
- Use customer-managed keys to control encryption keys for data at rest Finance & Operations (http://learn.microsoft.com/dynamics365/fin-ops-core/dev-itpro/sysadmin/customer-managed-keys) the Power Platform integration dependency and the Commerce / CSU caveat table.
- Access controls for Dataverse and Power Platform (https://learn.microsoft.com/en-us/azure/azure-sovereign-clouds/public/access-controls-dataverse-power-platform) Azure sovereign clouds documentation links CMK explicitly to sovereignty and residency.
- Power Platform Well-Architected (https://learn.microsoft.com/en-us/power-platform/well-architected/security/encryption) Recommendations for data encryption.
- About data encryption (https://learn.microsoft.com/en-us/power-platform/admin/about-encryption) Power Platform admin.
- Community blog: Dataverse customer-managed key with Azure Key Vault key versioning (community.dynamics.com) for the on-demand key rotation detail.

> This is what the documentation shows. If you have hands-on experience that says otherwise, I'd genuinely like to hear it.
>
> Working through a data sovereignty decision in your Dynamics 365 environment? We're happy to think it through with you.
>
> 365connect.tech