

19.08.2026

Power Encrypt

Die Cloud nutzen, den Schlüssel
behalten

**Kundenseitige Verschlüsselung für
besonders schützenswerte Daten in
der öffentlichen Verwaltung**



Agenda

- Cloud und Datenhoheit in der öffentlichen Verwaltung
- **Praxisbeispiel:** Cloud-Migration einer kantonalen Fachanwendung
- Die technische Herausforderung
- Kundenseitige Verschlüsselung mit Power Encrypt
- Fragen und Diskussion

Cloud nutzen – Datenhoheit behalten



Cloud nutzen

- Innovation
- Skalierbarkeit
- Moderne Cloud-Dienste

Muss sich die
öffentliche
Verwaltung
entscheiden?



Datenhoheit behalten

- Besonders schützenswerte Personendaten
- Gesetzliche Geheimhaltungspflichten
- Eigene Schlüsselkontrolle

Cloud-Souveränität wird zur Schlüsselfrage

- **Datenstandort ≠ Datenhoheit**
Ein Schweizer Speicherort allein schliesst Zugriffe aufgrund ausländischer Rechtsordnungen nicht aus.
- **Besonders schützenswerte Personendaten**
Öffentliche Organe müssen Datenschutz, Geheimhaltung und Risiken der Cloud-Auslagerung berücksichtigen.
- Entscheidend ist die Kontrolle
Wer kann technisch auf die Daten zugreifen – und wer kontrolliert die Schlüssel?

→ privatim konkretisiert diese Anforderung für öffentliche Organe.

privatim: Cloud-Anbieter ohne Zugang zum Schlüssel

«... wenn die Daten vom verantwortlichen Organ selbst verschlüsselt werden und der Cloud-Anbieter keinen Zugang zum Schlüssel hat.»

Quelle: privatim, Resolution zur Auslagerung von Datenbearbeitungen in die Cloud, 24.11.2025



Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des Préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Fazit: Die Nutzung internationaler SaaS-Lösungen für besonders schützenswerte oder einer gesetzlichen Geheimhaltungspflicht unterstehende Personendaten durch öffentliche Organe ist nur dann möglich, wenn die Daten vom verantwortlichen Organ selbst verschlüsselt werden und der Cloud- Anbieter keinen Zugang zum Schlüssel hat.

Praxisbeispiel: Cloud-Migration einer kantonalen Fachanwendung

Ausgangslage



- Kantonale Verwaltung
- Dynamics 365 heute On-Premises
- Migration in die Microsoft Cloud wird geprüft

Herausforderung



- Besonders schützenswerte Personendaten
- Hohe Datenschutz- und Souveränitätsanforderungen
- Schlüssel unter eigener Kontrolle

Fragestellung



Wie lässt sich die Fachanwendung in die Cloud migrieren, ohne die Kontrolle über sensible Daten aufzugeben?

Was ist “falsch” an der Cloud?

Hyperscaler **binden sich konzeptbedingt selbst in die Vertrauenskette** ein.

Cloud-Plattformen bieten zwar modernste Innovationen und ein sehr hohes Sicherheitsniveau, doch man muss dabei in Kauf nehmen, dass die **Anbieter Zugriff auf die eigenen Daten** haben.

Für viele Kunden – **insbesondere im öffentlichen Sektor** – ist dies oft ein entscheidendes Ausschlusskriterium.

Für diese Kunden gibt es nur wenige Optionen:

- Sie **bleiben on-premises**, mit der Konsequenz, weniger innovativ zu sein
- Sie nutzen **private Clouds** und **Open-Source-Software**, welche nur schwer mit den globalen Cloud Lösungen konkurrenzieren können.

Aber es gibt eine weitere Option...

Kontextualisierung

Beispiel anhand von Dynamics 365

Nachfolgender Inhalt bezieht sich auf die Nutzung von Dynamics 365 mit Power Encrypt.
Dies dient lediglich der Veranschaulichung, gilt aber auch für weitere Applikationen.

LS1

Added by LSG

Lloyd SEBAG; 2026-08-14T07:41:16.985

Dynamics 365: Was ist geschützt – und wo bleibt die Lücke?

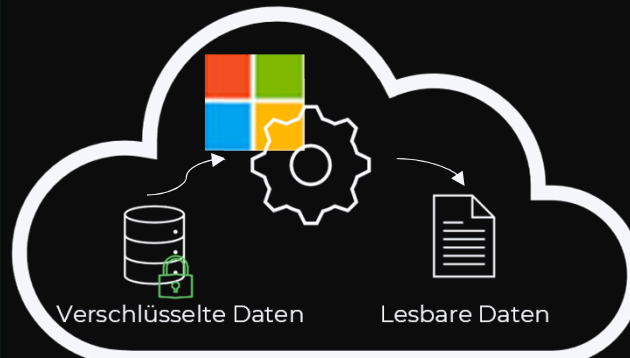
Übertragung



☒ Geschützt

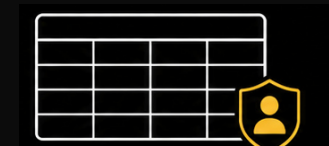
TLS schützt die Übertragung zwischen Benutzer und der Cloud

Speicherung



Die von Microsoft angebotene Verschlüsselung gilt nur für die Datenbankdatei selbst und nicht für die Daten innerhalb der Datenbank (SQL TDE). Daher bleiben alle Daten für Microsoft und seine Dienste im Klartext lesbar.
LS1
 (auch bei BYOK/ CMK, siehe nächste Folie)

Zugriff auf Felder



In Dynamics 365 gibt es keine Verschlüsselung auf Zellenebene, **LS2**er verhindert werden könnte, dass Microsoft die Daten einsehen kann.

Folie 9

LS1 Must be readable BY MICROSOFT. Important to say it clearly like that if you can add :)

Lloyd SEBAG; 2026-08-17T13:00:06.163

LS2 ??

Lloyd SEBAG; 2026-08-17T13:00:25.804

BYOK & CMK ≠ HYOK

Analogie «Bankschliessfach» (vereinfacht)

Standard

Die Bank hat den Schlüssel zum Schloss



BYOK / CMK

Eigenes Schloss und eigener Schlüssel, welcher die Bank aufbewahrt

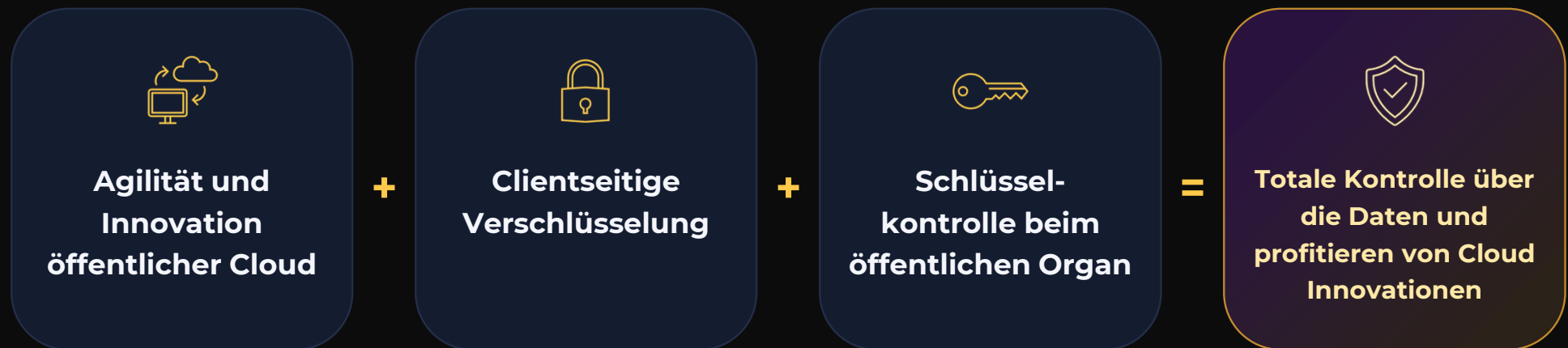


HYOK

Eigenes Schloss und eigener Schlüssel, die Bank hat **nie** den Schlüssel



Die Gleichung der Datensouveränität



Paradigmenwechsel: Wir müssen uns von einer blinden Abhängigkeit von globalen Plattformen hin zu absoluter kryptografischer Unabhängigkeit (Sovereignty by Design) bewegen.

Die Lösung



Power Encrypt

LS1

Added by LSG

Lloyd SEBAG; 2026-08-14T07:42:47.640

Was ist Power Encrypt?



Sofortige Ver- und Entschlüsselung, für die Benutzer transparent. Basierend auf den höchsten Sicherheitsstandards.



Sicherer Schlüsselverwaltungsprozess über das Admin Center.



Möglichkeit, sensible Daten gemäss der Datenklassifizierung des Kunden zu definieren.



Kompatibel mit allen Arten von Anwendungen. Plug-and-Play-Konnektoren für gängige Anwendungen wie Dynamics 365, SharePoint und viele andere verfügbar.



Verschiedene Betriebsmodi verfügbar. Unterstützung für die Integration mit anderen Systemen, Portalen usw.



Data Shield. Überwachen Sie die Nutzung. Erkennen und reagieren Sie auf verdächtiges Verhalten. Verwalten Sie Benutzer und vieles mehr.



Die Suchfunktion wurde beibehalten und durch eine Fuzzy-Suchoption sogar verbessert.

LS1

Added by LSG

Lloyd SEBAG; 2026-08-14T07:43:18.557

Wie funktioniert Power Encrypt technisch?

Clientseitig verschlüsseln



- Sensible Daten werden vor der Speicherung in der Cloud verschlüsselt.
- Für geschützte Felder erhält die Cloud nur verschlüsselte Werte.

Schlüssel selbst kontrollieren



- Die Schlüssel bleiben unter Kontrolle des Kunden bzw. des öffentlichen Organs.
- Der Cloud-Anbieter erhält keinen Zugriff auf den Schlüssel um die Daten zu entschlüsseln

Transparent nutzen



- Autorisierte Benutzer sehen die Daten im Frontend im Klartext.
- Bestehende Anwendungen und Geschäftsprozesse können weiter genutzt werden.

Schutzprinzip

Klartext entsteht nur auf der autorisierten Seite – im Cloud-Backend bleiben sensible Daten verschlüsselt.

Was sieht die Cloud – ohne und mit Power Encrypt?

Dataverse Backend SQL Store

```
select top 1 firstname, lastname from contact
order by createdon desc
```

Dynamics 365 CRM / Front UI

Dataverse Backend SQL Store

```
select top 1 firstname, lastname from contact
order by createdon desc
```

Dynamics 365 / Power Apps Front UI

Sensible Daten sind im Backend im Klartext lesbar.

Im Backend verschlüsselt – für autorisierte Benutzer im Frontend weiterhin lesbar.

LS1

Why this one ? As you are spoiling what will come on the videos.. ? Is that for the light version ?

Lloyd SEBAG; 2026-08-14T07:47:13.638

Ohne Power Encrypt (Demo Video)

The screenshot displays the Dynamics 365 interface. On the left, a SQL query execution window is open, showing a query to select the top 1 contact by creation date. The query is: `select top 1 firstname, lastname from contact order by createdon desc`. The results pane below the query is empty, showing columns for 'firstname' and 'lastname'. The status bar at the bottom of the query window indicates '0 rows'.

On the right, the 'My Active Contacts' view is shown. The view is currently empty, displaying a message: 'We didn't find anything to show here'. The view includes a search bar labeled 'Filter by keyword' and a table with columns for 'Full Name', 'Email', and 'Company'. The status bar at the bottom of the view indicates 'Rows: 0'.

The Dynamics 365 navigation pane on the left includes sections for Engagement (Get started, Journeys, Analytics, Triggers, Campaigns), Audience (Segments, Contacts, Consent center), and Channels (Real-time journeys).

Mit Power Encrypt (Demo Video)

The screenshot displays a Power Apps application interface. On the left, a table titled 'Results' shows columns for 'LastName', 'FirstName', and 'SensitiveData'. The main area is titled 'Active Custom Contacts*' and features a table with the same columns. The top navigation bar includes 'Power Apps' and 'SANDBOX'. A sidebar on the left contains navigation links: Home, Recent, Pinned, and Custom Contacts. The bottom of the interface shows a 'Contact Us' link and the website 'powerencrypt.io'.

Dataverse Backend SQL Store

Dynamics 365 / Power Apps Front UI

Verschiedene Webanwendungen integrierbar

Plugins

Power Encrypt enthält
einsatzbereite Plugins für
verschiedene beliebte
Anwendungen.

Modular

Weitere Webanwendungen
können in Power Encrypt
integriert werden



ORACLE®



Praxisbeispiel: Sichere Cloud-Migration einer kantonalen Fachanwendung

Eine kantonale Verwaltung prüfte die Migration einer bestehenden Dynamics-365-Fachanwendung in die Microsoft Cloud. Wegen besonders schützenswerter Personendaten und hohen Souveränitätsanforderungen wurde Power Encrypt als mögliche Lösungsvariante evaluiert.




Technische Eckpunkte
Batch-Server bleibt bestehen und wird über das Power-Encrypt-SDK angebunden. Schlüsselmanagement und Client-Komponenten verbleiben unter Kontrolle des Kantons.



Wichtige Einordnung
Power Encrypt wurde im Rahmen des Migrationsvorhabens evaluiert und offeriert. Eine produktive Einführung war zum damaligen Zeitpunkt noch nicht beschlossen.

Fragen & Diskussion

Cloud-Souveränität, Schlüsselkontrolle und Einsatz in der öffentlichen Verwaltung

Vielen Dank



Fabian Kalchofner

Senior Expert

fabian.kalchofner@elca.ch



Janos Tolcsvai

Senior Client Partner

janos.tolcsvai@elca.ch

www.powerencrypt.io

admin@powerencrypt.io