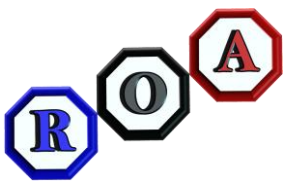




Power Pages im Enterprise-Einsatz: Kosten, Compliance und Kontrolle im Griff

Power Pages strategisch führen: So sichern Sie Ihre Daten im Microsoft-Ökosystem, erfüllen die DSGVO-Vorgaben und behalten die volle Kontrolle über Lizenzen und IT-Wildwuchs.

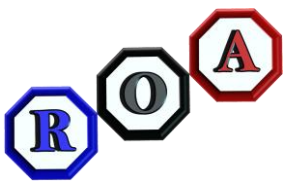
Ein Whitepaper von Volker Buntrock



Power Pages im Enterprise-Einsatz: Kosten, Compliance und Kontrolle im Griff

Inhaltsverzeichnis

Executive Summary	2
Einleitung: Zwischen Agilität und Kontrolle.....	4
Kostenkontrolle & Lizenzmanagement.....	5
IT-Governance & Wildwuchs-Prävention	7
Sicherheit auf Enterprise-Niveau	9
Recht & Compliance (DSGVO-Fokus)	11
Der strategische Fahrplan (Checkliste).....	13
Fazit: Power Pages als strategischer Wettbewerbsvorteil	15



Executive Summary

Problem:

Im Enterprise-Umfeld entstehen bei Power Pages schnell versteckte Kosten und organisatorische Risiken: falsch gewählte Lizenzmodelle, ineffiziente Dataverse-Speichernutzung, unkontrollierter Wildwuchs in den Umgebungen sowie unsaubere Governance- und Sicherheitskonzepte. Dazu kommt der Druck, DSGVO- und Compliance-Vorgaben lückenlos einzuhalten. Ohne klare Steuerung wächst die Plattform schneller als ihre Kontrolle – mit der Folge steigender Kosten, Sicherheitslücken und intransparenter Verantwortlichkeiten.

Kernpunkt:

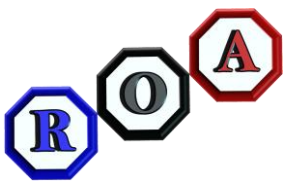
Der eigentliche Hebel liegt nicht in der technologischen Umsetzung eines Portals, sondern in der strategischen Führung der Plattform: sauberes Lizenzmanagement, kontrollierte Datenströme, DLP-Richtlinien, Environment-Struktur, ein durchdachtes Berechtigungskonzept und die klare Zuordnung von Verantwortlichkeiten. Power Pages entfaltet seine Stärke erst dann, wenn Kosten, Sicherheit und Governance aktiv gesteuert werden – nicht als IT-Bremse, sondern als produktives Betriebsmodell.

Mehrwert:

Mit einem fundierten Governance-Setup wird Power Pages zum skalierbaren Enterprise-Werkzeug: transparente Kostenkontrolle, kontrollierte Datenflüsse, revisionsfähige Zugriffe, abgesicherte Authentifizierung über Entra ID, integrierte WAF-Abwehrmechanismen und volle regionale Datenhoheit im Microsoft-Ökosystem. Die IT behält Sicherheit und Compliance im Griff, während die Fachbereiche schnell und flexibel Kunden- und Partnerportale bereitstellen können. Innovation mit Leitplanken – statt Schatten-IT ohne Überblick.

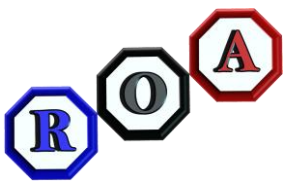
Risiko ohne Struktur:

Ohne klare Steuerung drohen explodierende Lizenzkosten, unkontrollierte Dataverse-Speicherlast, Sicherheitsrisiken durch falsch konfigurierte Portale, DLP-Verstöße, fehlende DSGVO-Nachweisbarkeit und eine wachsende Schatten-IT. Fachabteilungen erstellen Portale ohne



Power Pages im Enterprise-Einsatz: Kosten, Compliance und Kontrolle im Griff

IT-Einbindung, während Compliance, Datenlöschung und Audit-Trails unzureichend umgesetzt bleiben. Fehlende Standards führen langfristig zu chaotischen Portal-Landschaften und teuren Altlasten – technisch, organisatorisch und finanziell.



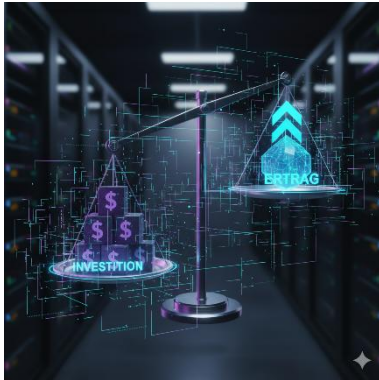
Einleitung: Zwischen Agilität und Kontrolle

Microsoft Power Pages hat das Versprechen der digitalen Transformation für viele Unternehmen eingelöst: Noch nie war es so einfach, geschäftskritische Daten sicher in das World Wide Web zu verlängern. Doch wo die Fachabteilungen enorme Geschwindigkeitsvorteile bei der Bereitstellung von Kunden- und Partnerportalen sehen, blickt die IT-Leitung oft mit Sorge auf eine wachsende Schatten-IT, komplexe Lizenzmodelle und die Frage der DSGVO-Konformität.

Wer Power Pages im Enterprise-Umfeld einsetzt, merkt schnell: Die Erstellung der Oberfläche ist nur die Spitze des Eisbergs. Die wahre Herausforderung liegt unter der Wasseroberfläche – in der strategischen Führung der Plattform. Ein Portal, das technisch in wenigen Tagen steht, kann ohne ein fundiertes Governance-Modell und eine saubere Kostenplanung langfristig zur organisatorischen Belastung werden.

In diesem Guide verlassen wir die Ebene der bunten Kacheln und Design-Vorlagen. Wir werfen einen nüchternen Blick auf die harten Fakten: Wie steuern Sie die Kosten für authentifizierte Nutzer? Wie sichern Sie den Zugriff auf Ihr Dataverse ab, ohne die Benutzerfreundlichkeit zu opfern? Und wie stellen Sie sicher, dass Ihre Portale nicht nur heute funktionieren, sondern auch morgen noch den strengen rechtlichen Anforderungen Ihres Unternehmens entsprechen.

Kostenkontrolle & Lizenzmanagement



Wer die Power Platform einführt, stellt sich unweigerlich die Frage: „Wird das am Ende teurer als eine Individualentwicklung?“ Die Antwort bei Power Pages hängt massiv davon ab, wie präzise Sie die Nutzergruppen definieren. Im Gegensatz zu klassischen SaaS-Modellen rechnet Microsoft hier nicht nach „Seats“, sondern nach **Interaktion**.

Das Lizenzmodell: Authentifiziert vs. Anonym

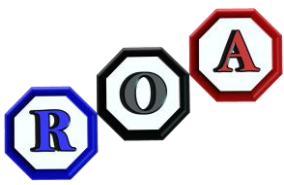
Das Herzstück der Kostenplanung ist die Unterscheidung der Zugriffsart. Hier entscheiden oft Nuancen über vier- bis fünfstellige Beträge im Jahresbudget:

- **Authentifizierte Benutzer (per User/Month):** Dies ist die Wahl für Partnerportale oder Kundenbereiche, in denen sich Nutzer einloggen (z. B. über Entra ID, LinkedIn oder B2C). Abgerechnet wird pro eindeutigem Benutzer, der sich innerhalb eines Monats anmeldet.
 - *Strategischer Tipp:* Nutzen Sie dieses Modell für Portale mit hoher Bindung, aber überschaubarer Nutzerzahl.
- **Anonyme Benutzer (per Website/Month):** Ideal für öffentliche Informationsportale oder Antragsstrecken ohne Login. Hier zahlen Sie für die Anzahl der monatlichen Seitenbesucher.
 - *Strategischer Tipp:* Achten Sie auf Skaleneffekte. Bei hohen Besucherzahlen sinken die Kosten pro Kopf durch Mengenrabatte (Tier-Pricing) drastisch.

Dataverse-Consumption: Der heimliche Kostentreiber

Ein häufiger Fehler in der Kalkulation ist das Ignorieren des **Dataverse-Speichers**. Jede Power Page schreibt Daten in das Dataverse.

1. **Datenbank-Kapazität:** Jede Interaktion verbraucht Speicher.



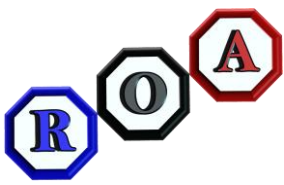
2. **Datei-Kapazität:** Hochgeladene PDFs von Kunden (z. B. bei Anträgen) landen oft im teuren Dataverse-Speicher statt in einem günstigen Azure Blob Storage.
3. **Log-Dateien:** Audit-Logs für die Compliance können den Speicher schleichend füllen.

Pay-as-you-go vs. Prepaid-Kapazität

Für Entscheider bietet Microsoft zwei Wege:

- **Prepaid (Capacity Add-ons):** Sie kaufen Pakete (z. B. 100 Nutzer) im Voraus. Das ist günstig, erfordert aber eine genaue Prognose.
- **Pay-as-you-go (über Azure Subscription):** Sie zahlen nur das, was wirklich genutzt wurde. Ideal für die Pilotphase oder saisonale Schwankungen, aber im Grundpreis pro Einheit etwas teurer.

*Starten Sie mit einem **Pay-as-you-go-Modell**, um echte Nutzungsdaten zu sammeln. Sobald sich das Besucherverhalten stabilisiert, wechseln Sie in die Prepaid-Modelle, um von den Rabattstaffeln zu profitieren. Achten Sie strikt darauf, dass Anhänge (Files) nicht das teure Dataverse verstopfen, sondern konsequent nach Azure ausgelagert werden.*



IT-Governance & Wildwuchs-Prävention

Die größte Sorge vieler IT-Leiter bei der Einführung von Low-Code-Plattformen ist der sogenannte „Wildwuchs“. Ohne klare Leitplanken entstehen hunderte isolierte Portale, die niemand mehr wartet, deren Sicherheitsstand veraltet und deren Datenqualität zweifelhaft ist. Governance ist hier kein Hindernis, sondern der Enabler für eine sichere Skalierung.

Die Environment-Strategie: Ordnung von Anfang an

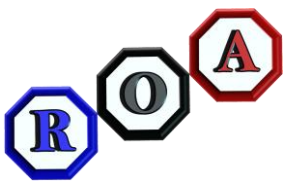
Ein klassischer Fehler ist die Nutzung der „Default-Umgebung“ für produktive Portale. Für eine saubere Governance ist eine strikte Trennung Pflicht:

- **Entwicklungs-Umgebung:** Hier dürfen Maker experimentieren.
- **Test/QA-Umgebung:** Validierung von Design, Prozessen und Berechtigungen.
- **Produktions-Umgebung:** Streng reglementiert, Zugriff nur für finale Releases.
- *Strategischer Vorteil:* Durch dedizierte Umgebungen stellen Sie sicher, dass Experimente der Fachabteilungen niemals die Stabilität Ihrer Live-Systeme gefährden.

Managed Environments & DLP-Richtlinien

Microsoft bietet mit den **Managed Environments** ein Werkzeugset, um die Kontrolle zu automatisieren. Das wichtigste Instrument sind die **Data Loss Prevention (DLP) Richtlinien**:

- Sie legen fest, welche Konnektoren miteinander kommunizieren dürfen.
- *Beispiel:* Sie können verhindern, dass Daten aus Ihrem Dataverse (z. B. Kundendaten) versehentlich durch einen schlecht konfigurierten Workflow an private Cloud-Speicher oder soziale Medien gesendet werden.



Maker-Enablement: Freiheit mit Leitplanken

Governance bedeutet nicht, alles zu verbieten. Es geht um ein „Center of Excellence“ (CoE):

1. **Zentrales Register:** Jede Power Page muss einen verantwortlichen Owner und einen klaren Business-Case haben.
2. **Archivierung:** Portale, die über einen Zeitraum von X Monaten keine Zugriffe verzeichnen, werden automatisch zur Löschung vorgeschlagen.
3. **Branding-Templates:** Geben Sie Vorlagen vor, damit jedes Portal automatisch dem Corporate Design entspricht – das spart Review-Schleifen.

Der „Shadow IT“-Check

Durch das Power Platform Admin Center behalten Sie die volle Sichtbarkeit. Sie sehen auf Knopfdruck, wer welche Portale erstellt hat und wer darauf zugreift. Für Entscheider ist diese Transparenz die Versicherung gegen unkontrollierte Kosten und Sicherheitsrisiken.

Governance bei Power Pages ist kein administratives Monster, sondern die notwendige Struktur für Geschwindigkeit. Etablieren Sie eine **Drei-Instanzen-Landschaft** (Dev/Test/Prod) und setzen Sie **DLP-Richtlinien** konsequent um. So ermöglichen Sie Innovation in den Fachabteilungen, ohne die Hoheit über Ihre Datenarchitektur zu verlieren.

Sicherheit auf Enterprise-Niveau



Jede Power Pages Instanz ist von Haus aus gegen die gängigsten Bedrohungen geschützt. Durch die Integration von **Azure Front Door** und der **Web Application Firewall (WAF)** wird Ihr Portal aktiv verteidigt gegen:

- **DDoS-Attacken:** Überlastungsangriffe werden abgefangen, bevor sie Ihre Geschäftslogik erreichen.
- **SQL-Injection & Cross-Site Scripting:** Die Firewall erkennt und blockiert bösartige Eingabemuster in Echtzeit.

Identitätsmanagement: Wer darf rein?

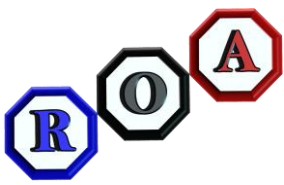
Ein entscheidender Sicherheitsfaktor ist die Kontrolle darüber, wer sich anmeldet. Power Pages nutzt moderne Industriestandards:

- **Integration von Microsoft Entra ID (Azure AD):** Nutzen Sie vorhandene Identitäten für Mitarbeiter oder Partner.
- **Azure AD B2C:** Für Kundenportale mit Millionen von Nutzern bietet dies Multi-Faktor-Authentifizierung (MFA) und Schutz vor Brute-Force-Angriffen.
- **Externe Identitäten:** Auch soziale Logins (Google, LinkedIn) können sicher angebunden werden, wobei die Datenhoheit immer in Ihrem Dataverse bleibt.

Das Prinzip der geringsten Berechtigung (Least Privilege)

Die Sicherheit im Inneren wird über das **Dataverse-Sicherheitsmodell** gesteuert. Anders als bei einfachen CMS-Systemen können Sie auf Zeilenebene festlegen, was ein Nutzer sieht:

- **Tabellenberechtigungen:** Ein Kunde sieht nur seine eigenen Rechnungen, niemals die eines anderen Kunden.
- **Spalten-Sicherheit:** Sensible Felder (z. B. interne Kommentare) bleiben für den externen Nutzer unsichtbar, selbst wenn er Zugriff auf den restlichen Datensatz hat.



Verschlüsselung und Compliance

Alle Daten sind sowohl während der Übertragung (**In Transit**) via TLS 1.2+ als auch im Speicher (**At Rest**) verschlüsselt. Dies ist die Grundvoraussetzung, um in regulierten Branchen überhaupt über Cloud-Lösungen nachdenken zu dürfen.

Sicherheit bei Power Pages ist kein „Add-on“, sondern ein integraler Bestandteil der Architektur. Durch die Nutzung von **Entra ID** und der **Web Application Firewall** delegieren Sie die komplexesten Sicherheitsaufgaben an Microsoft. Ihre Aufgabe als Entscheider ist es, sicherzustellen, dass das **Berechtigungskonzept im Dataverse** sauber definiert ist – die technische Schutzmauer drumherum steht bereits.

Recht & Compliance (DSGVO-Fokus)



In Zentraleuropa ist die Einhaltung von Datenschutzvorgaben (DSGVO in der EU, revDSG in der Schweiz) nicht verhandelbar. Ein häufiges Vorurteil gegenüber Cloud-Lösungen ist die Sorge um den Datenstandort. Bei Power Pages lässt sich dieses Risiko durch die gezielte Wahl der Rechenzentren vollständig beherrschen.

Regionale Datensouveränität: Sie entscheiden, wo die Daten liegen

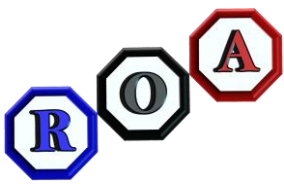
Microsoft betreibt spezifische Rechenzentrumsregionen, die es Ihnen ermöglichen, nationale und europäische Compliance-Vorgaben exakt einzuhalten:

- **Österreich & Deutschland:** Nutzen Sie Regionen wie „Germany West Central“ (Frankfurt) oder die Kapazitäten in Österreich, um sicherzustellen, dass Daten das EU-Rechtsterritorium nicht verlassen.
- **Schweiz & Liechtenstein:** Für Schweizer Unternehmen ist die Speicherung innerhalb der Landesgrenzen (z. B. Region „Switzerland North“ in Zürich) oft eine gesetzliche Bedingung. Power Pages unterstützt diese lokale Datenhaltung explizit.
- **Südtirol:** Durch die Nutzung europäischer Serverstandorte werden die italienischen Anforderungen an die DSGVO vollumfänglich erfüllt.

Transparenz durch Audit-Logs und Monitoring

Ein Kernaspekt der Compliance ist die Nachweisbarkeit. Power Pages bietet detaillierte Protokollierungsmöglichkeiten:

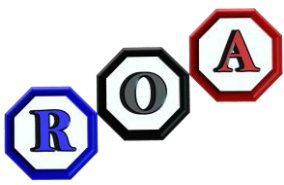
- **Zugriffskontrolle:** Wer hat wann auf welche Daten zugegriffen? Diese Audit-Logs sind für die interne Revision und externe



Power Pages im Enterprise-Einsatz: Kosten, Compliance und Kontrolle im Griff

Aufsichtsbehörden (wie die DSB in Österreich oder den EDÖB in der Schweiz) essenziell.

- **Datenlöschkonzepte:** Automatisierte Workflows sorgen dafür, dass Daten nach Ablauf von Aufbewahrungsfristen rechtssicher gelöscht werden.



Der strategische Fahrplan (Checkliste)

Ein Power-Pages-Projekt scheitert selten an der Technik, sondern meist an einer unklaren Roadmap. Für Entscheider ist es entscheidend, den Prozess von der ersten Idee bis zum produktiven Betrieb zu strukturieren. Nutzen Sie diesen 5-Punkte-Fahrplan als Blaupause für Ihre Umsetzung.

1. Die Definitionsphase: Problem vor Lösung

Bevor die erste Zeile Code geschrieben wird, muss feststehen:

- **Zielgruppe:** Wer greift zu? (Kunden, Partner oder Bürger?)
- **Datenmodell:** Welche Informationen aus dem Dataverse sind absolut notwendig? (Datenminimierung nach DSGVO).
- **Erfolgskennzahlen:** Woran messen wir den ROI? (z.B. Reduktion der Support-Anrufe um 20%).

2. Proof of Concept (PoC) – „Fail Fast or Scale Fast“

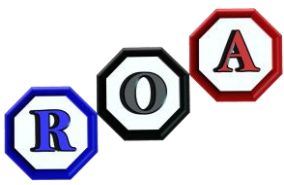
Starten Sie klein. Setzen Sie innerhalb von 2 bis 4 Wochen ein funktionales Pilot-Portal auf.

- **Fokus:** Nur eine Kernfunktion (z. B. eine Statusabfrage für Anträge).
- **Ziel:** Feedback von echten Nutzern einholen und die technische Machbarkeit der Integration prüfen.

3. Governance-Setup & Security-Check

Bevor das Portal für die Öffentlichkeit sichtbar wird, muss die IT-Abteilung die Infrastruktur härten:

- Einrichtung der **DLP-Richtlinien** (siehe Kapitel 2).
- Aktivierung der **Web Application Firewall**.
- Durchführung eines **Penetration-Tests** oder eines internen Security-Audits.



4. Das Rollout-Szenario

Ein „Big Bang“ ist selten ratsam. Empfehlenswert ist ein phasenweiser Rollout:

- **Phase 1:** Interner Betatest.
- **Phase 2:** Friendly-User-Test (ausgewählte Kunden/Partner).
- **Phase 3:** Globaler Go-Live.

5. Betrieb & Kontinuierliche Optimierung

Ein Portal ist ein lebendes Produkt. Planen Sie Ressourcen für die Wartung ein:

Monitoring: Überwachung der monatlichen Logins zur Kostenoptimierung (Lizenz-Check).

- **Updates:** Power Pages wird von Microsoft automatisch aktualisiert, aber Ihre individuellen Anpassungen sollten bei jedem Release kurz geprüft werden.

Geschwindigkeit ist der größte Vorteil von Power Pages – aber nur, wenn der Prozess stimmt. Nutzen Sie den **PoC-Ansatz**, um schnell Ergebnisse zu sehen, und investieren Sie erst in die volle Skalierung, wenn das Feedback der Nutzer und die Freigabe der IT-Security vorliegen.

Fazit: Power Pages als strategischer Wettbewerbsvorteil

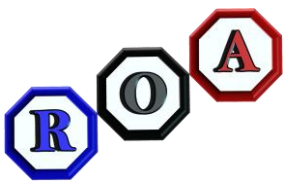


Die Entscheidung für Microsoft Power Pages ist weit mehr als die Wahl eines neuen Web-Tools – es ist die Entscheidung für eine **integrierte Datenstrategie**. Wie dieser Guide gezeigt hat, liegen die größten Vorteile in der nahtlosen Einbettung in das bestehende Microsoft-Ökosystem, kombiniert mit höchster regionaler Flexibilität.

Für Sie als Entscheider bedeutet das:

1. **Sicherheit durch Architektur:** Sie müssen das Rad nicht neu erfinden. Durch die Nutzung der Azure-Infrastruktur und des Dataverse-Sicherheitsmodells erhalten Sie eine Enterprise-Absicherung, die bei Individualentwicklungen oft unbezahlbare Ressourcen binden würde.
2. **Kosten als Stellschraube:** Das Lizenzmodell erfordert Aufmerksamkeit, bietet aber enorme Skalierbarkeit. Durch die präzise Steuerung von Zugriffen und die Vermeidung teurer Speicherfresser lassen sich die Total Cost of Ownership (TCO) im Vergleich zu klassischen Portallösungen signifikant senken.
3. **Governance als Beschleuniger:** Ordnung schafft Geschwindigkeit. Mit klaren Leitplanken (DLP-Richtlinien) und einer sauberen Environment-Strategie ermöglichen Sie Ihren Fachabteilungen Innovationen, ohne die Hoheit über Ihre Datenarchitektur zu verlieren.
4. **Compliance ohne Grenzen:** Ob DSGVO in Österreich, Südtirol und Liechtenstein oder das revDSG in der Schweiz – Power Pages ist kein Hindernis, sondern ein Enabler. Durch die gezielte Wahl der Rechenzentrums-Regionen (z. B. Frankfurt, Zürich oder Wien/Genf) stellen Sie sicher, dass Ihre Daten genau dort bleiben, wo sie hingehören.

Ihre nächsten Schritte: Bleiben Sie nicht in der Planungsphase stecken. Starten Sie mit einem fokussierten Pilotprojekt (PoC), validieren



Power Pages im Enterprise-Einsatz: Kosten, Compliance und Kontrolle im Griff

Sie die Kosten-Nutzen-Rechnung anhand echter Daten und skalieren Sie dann auf Basis eines festen Governance-Fundaments.

Power Pages bietet Ihnen die Chance, die Lücke zwischen den hohen IT-Anforderungen und dem Innovationsdrang der Fachbereiche zu schließen – rechtssicher, kalkulierbar und technologisch führend für Ihr gesamtes Marktgebiet.