Dracoon: Sichere Datenhoheit für smarte Unternehmen

Category: Online-Marketing
geschrieben von Tobias Hager | 5. Februar 2026

Dracoon: Sichere Datenhoheit für smarte

Unternehmen

Cloud ist geil – bis deine Daten plötzlich in Kalifornien statt Karlsruhe liegen. Wer 2024 noch blind auf US-Dienste setzt, hat entweder die DSGVO nicht verstanden oder seine Kunden nicht ernst genommen. Willkommen im Zeitalter der digitalen Souveränität – und im Zentrum steht: Dracoon. In diesem Artikel zeigen wir dir, warum Dracoon nicht bloß ein weiterer Filehoster ist, sondern die letzte Bastion echter Datenhoheit für Unternehmen, die mehr wollen als Buzzwords und bunte Dashboards.

- Was Dracoon wirklich ist – und warum es mehr als ein Cloud-Speicher ist
- Wie Dracoon echte Datenhoheit ermöglicht – technisch und rechtlich
- Zero Knowledge Encryption erklärt – und warum sie dich wirklich schützt
- Die Unterschiede zu Dropbox, Google Drive & Co. – Feature für Feature
- Warum Dracoon für DSGVO, ISO 27001 und BSI-Vorgaben ein No-Brainer ist
- API-first: Wie sich Dracoon nahtlos in deine IT-Landschaft integriert
- Use Cases: Vom Mittelstand bis zur Enterprise – wer Dracoon wie nutzt
- On-Premise, Private Cloud oder SaaS – wie du Dracoon betreiben kannst
- Fallstricke bei der Einführung – und wie du sie vermeidest
- Fazit: Warum echte Datenkontrolle kein Luxus, sondern Pflicht ist

Dracoon erklärt: Mehr als nur ein sicherer Cloud-Speicher

Dracoon ist nicht einfach ein weiterer Cloud-Dienst mit hübscher UI und versprochenem Datenschutz. Es ist eine Plattform für Enterprise File Services, die Sicherheit, Compliance und Integrationsfähigkeit auf ein Niveau hebt, das den meisten US-Diensten schlicht fehlt. Hinter dem Namen steckt ein deutsches Unternehmen, das sich seit Jahren auf eines spezialisiert hat: maximale Kontrolle über sensible Daten.

Im Gegensatz zu Dropbox, OneDrive oder Google Drive ist Dracoon von Grund auf auf Security und Integrität ausgelegt. Das beginnt mit einer Ende-zu-Ende-Verschlüsselung, die nicht nur verschlüsselt, sondern Zero Knowledge bedeutet. Der Clou daran: Nicht einmal Dracoon selbst kann auf die Inhalte zugreifen. Die Schlüsselverwaltung liegt komplett in deiner Hand.

Die Plattform ist ISO 27001 zertifiziert, BSI-C5-konform und wird regelmäßig extern auditiert. Und ja, die Server stehen in Deutschland – ein entscheidender Unterschied für alle, die unter der DSGVO arbeiten (müssen). Denn während amerikanische Anbieter durch den CLOUD Act verpflichtet sind, auf Anfrage Zugriff zu gewähren, bleibt Dracoon juristisch unangreifbar.

Dracoon ist modular aufgebaut und API-first. Das bedeutet: Du kannst die Plattform vollständig in deine bestehende IT-Landschaft integrieren – von Microsoft 365 über SAP bis zu individuellen Systemen. Die Rollen- und Rechteverwaltung ist granular, mandantenfähig und auditierbar. Kurz gesagt: Dracoon ist keine Cloud-Spielwiese, sondern ein Werkzeug für Profis.

Datenhoheit durch Zero Knowledge – was das technisch bedeutet

Der Begriff „Datenhoheit“ wird im Marketing oft inflationär genutzt – meist ohne echten technischen Unterbau. Bei Dracoon ist das anders. Die Plattform setzt auf ein Zero Knowledge Encryption-Modell, das sich fundamental von der Verschlüsselung bei anderen Anbietern unterscheidet. Hierbei wird der Schlüssel zur Entschlüsselung der Daten ausschließlich vom Kunden erzeugt und verwaltet – und eben nicht vom Anbieter.

Technisch bedeutet das: Alle Daten werden clientseitig verschlüsselt, bevor sie überhaupt das Gerät verlassen. Die Verschlüsselung erfolgt mit 256-Bit AES im GCM-Modus – einem Standard, der selbst militärischen Anforderungen genügt. Die Schlüssel wiederum werden durch ein passwortbasiertes Key Derivation Function (KDF) wie PBKDF2 erzeugt und niemals auf dem Server gespeichert.

Das Resultat: Selbst wenn jemand physischen Zugriff auf die Server hätte – etwa durch Einbruch, Gerichtsbeschluss oder Spionage – wären die Daten nutzlos. Ohne den Schlüssel, den nur der Kunde kennt, ist nichts zugänglich. Nicht einmal Dracoon selbst kann Entschlüsselung leisten. Zero Knowledge ist also nicht nur ein Buzzword, sondern gelebte Kryptographie.

Diese Architektur hat massive Vorteile – nicht nur für die Sicherheit, sondern auch für Compliance. Denn mit Zero Knowledge kann ein Unternehmen nachweisen, dass es technische und organisatorische Maßnahmen (TOMs) getroffen hat, um Daten vor unbefugtem Zugriff zu schützen – ein zentraler Punkt in der DSGVO.

Dracoon vs. Dropbox, OneDrive & Co: Ein technischer Vergleich

Viele Unternehmen nutzen nach wie vor US-basierte Dienste, weil sie bequem, günstig und bekannt sind. Doch diese Bequemlichkeit hat einen Preis – und der heißt Kontrollverlust. Dracoon bietet eine Reihe von Funktionen, die klassische Anbieter schlicht nicht leisten können oder wollen. Hier ein technischer Vergleich der wichtigsten Aspekte:

- Verschlüsselung: Dracoon bietet echte clientseitige Verschlüsselung mit Zero Knowledge. Dropbox & Co. verschlüsseln meist nur serverseitig – die Anbieter haben vollen Zugriff.
- Compliance: Dracoon ist DSGVO-konform, ISO 27001 zertifiziert, BSI-C5

geprüft. US-Dienste unterliegen dem CLOUD Act – ein Compliance-Albtraum.
- Hosting: Dracoon läuft auf deutschen Servern, optional auch on-premise. US-Dienste hosten in der Regel global, oft in den USA.
- API-Integration: Dracoon ist API-first. Du kannst alles – von Benutzerverwaltung bis Dateioperationen – automatisieren. Bei Dropbox & Co. sind APIs oft limitiert oder kostenpflichtig.
- Rollen- und Rechteverwaltung: Dracoon erlaubt granulare Rechtevergabe auf Benutzer-, Gruppen- und Raumebene. OneDrive kennt meist nur „kann lesen“ oder „kann bearbeiten“.
- Auditing & Logging: Dracoon protokolliert jede Aktion revisionssicher. Bei US-Diensten ist Logging oft intransparent oder gar nicht vorhanden.

Wenn du also glaubst, dass du mit Dropbox sicher arbeitest, solltest du dringend deine Hausaufgaben machen. Spätestens wenn ein Kunde oder Auditor genauer hinsieht, wird’s peinlich – oder teuer.

Integration, APIs und Deployment-Optionen: So flexibel ist Dracoon

Ein großer Vorteil von Dracoon ist seine technische Offenheit. Die Plattform wurde von Anfang an als API-first-System konzipiert. Das bedeutet: Jeder Aspekt der Plattform – von der Benutzerverwaltung über Dateizugriffe bis hin zu Sicherheitseinstellungen – ist über REST-APIs steuerbar. Für Unternehmen mit einer komplexen IT-Landschaft ist das Gold wert.

Die API ist sauber dokumentiert, versioniert und ermöglicht Integrationen mit Drittsystemen wie Microsoft 365, Salesforce, SAP, Nextcloud oder eigenen Backend-Systemen. Es gibt SDKs für Java, JavaScript, Python und mehr. Auch Webhooks und Event Trigger sind möglich, um Workflows zu automatisieren. Du willst bei Uploads automatisch ein Virus-Scan starten oder eine Mail verschicken? Kein Problem.

Dracoon bietet drei Betriebsmodelle:

- Public SaaS: Gehostet in deutschen Rechenzentren, vollständig gemanagt von Dracoon. Ideal für Unternehmen ohne eigene IT-Infrastruktur.
- Private Cloud: Eigene Instanz in deiner Cloud, z. B. auf AWS, Azure oder OpenStack. Volle Kontrolle bei optimalem Support.
- On-Premise: Installation in deinem eigenen Rechenzentrum. Maximale Souveränität, ideal für hochsensible Daten oder regulierte Branchen.

Durch diese Flexibilität kannst du Dracoon genau so betreiben, wie es deine Compliance, IT-Ressourcen und Sicherheitsanforderungen verlangen. Das macht die Plattform sowohl für KMUs als auch für Konzerne hochattraktiv.

Use Cases & Fallstricke – und wie du sie meisterst

Dracoon wird branchenübergreifend eingesetzt: von Kanzleien über Banken bis zu Industrieunternehmen. Typische Anwendungsfälle sind:

- Datenaustausch mit externen Partnern ohne Sicherheitsrisiko
- Compliance-gerechte Ablage sensibler Dokumente
- Integration in DMS-/ECM-Systeme
- Automatisierter Datenimport/-export via API
- Mobiler, aber sicherer Zugriff auf Unternehmensdaten

Aber Achtung: Auch bei Dracoon ist nicht alles Plug-and-Play. Typische Stolpersteine sind:

- Fehlende Key-Management-Strategie: Wer Zero Knowledge will, muss auch Schlüssel sicher verwalten können – idealerweise mit HSM oder Key Vault.
- Unklare Rechtekonzepte: Ohne saubere Rollenstruktur wird das Rechtemanagement schnell zum Chaos.
- API-Overhead: Wer Integrationen plant, braucht Entwicklerressourcen – sonst bleibt’s beim Wunsch.

Die gute Nachricht: Mit der richtigen Projektplanung und einem klaren Zielbild lassen sich diese Hürden souverän meistern. Und dann profitierst du von einer Plattform, die nicht nur sicher ist – sondern dir endlich wieder Kontrolle über deine Daten gibt.

Fazit: Dracoon ist nicht nett – sondern notwendig

Cloud-Speicher gibt’s wie Sand am Meer. Aber echte Datenhoheit ist selten. Dracoon liefert genau das – technisch sauber, rechtlich unangreifbar und operativ flexibel. Für Unternehmen, die ihre Daten nicht in fremde Hände geben wollen (oder dürfen), ist Dracoon keine Option, sondern Pflicht.

Wer heute noch auf Anbieter setzt, deren Geschäftsmodell auf Datenauswertung, US-Recht und Intransparenz basiert, handelt fahrlässig. Mit Dracoon bekommst du nicht nur ein Werkzeug, sondern eine Strategie – für Sicherheit, für Compliance und für digitale Souveränität. Und das, verdammt nochmal, ist 2024 nicht optional, sondern überlebenswichtig.