enclaive

HKN

Whitepaper

Datenschutz & Souveränität: Microsoft 365, Nextcloud & Managed Confidential Nextcloud im Vergleich

Executive Summary

Digitale Zusammenarbeit ist heute ein strategischer Kernprozess nahezu aller Organisationen. Collaboration-Tools bieten den Vorteil gemeinsamer Datenablagen, dem Arbeiten an Shared Documents und ergänzen dies durch Kommunikationsfunktionen wie Chat oder Video-Meetings.

Neben Funktionalität und Verfügbarkeit rücken jedoch Datenschutz und Datensouveränität zunehmend in den Mittelpunkt – nicht zuletzt angesichts regulatorischer Anforderungen, steigender Risiken internationaler Datenübermittlungen und der Notwendigkeit, die Kontrolle über sensible Informationen zu behalten.

Dieses Whitepaper vergleicht Microsoft 365, eine klassische Nextcloud-Installation sowie eine Managed Confidential Nextcloud auf Basis der Confidential-Computing-Technologie von enclaive. Der Fokus liegt ausschließlich auf den Aspekten der DSGVO-Konformität und der digitalen Souveränität. Der Vergleich bezieht sich dabei nur auf SaaS-Lösungen (Software-as-a-Service), da Microsoft 365 keine On-Premises-Variante unterstützt.

1 Einleitung

Unternehmen und öffentliche Einrichtungen stehen vor der Herausforderung, ihre digitale Zusammenarbeit so zu gestalten, dass sie strengsten Compliance-Anforderungen in Bezug auf Datenschutz und Informationssicherheit gerecht wird. Im Zentrum stehen dabei Plattformen für Datenaustausch und Kollaboration, die neben zuverlässiger Performance vor allem nachweisbare Rechtskonformität und robuste Sicherheitsmechanismen für die Datenvertraulichkeit mitbringen.

Regulatorische Vorgaben wie die DSGVO, EuGH-Urteile wie Schrems-II oder US-Gesetze wie der CLOUD Act – die US-Behörden erlauben, auch in Europa gehostete Daten europäischer Organisationen von US-Unternehmen anzufordern – stecken den allgemeinen rechtlichen Rahmen klar ab. Darüber hinaus gilt es in vielen Branchen, zusätzliche Anforderungen und Regelwerke zu berücksichtigen, um lückenlose Auditierbarkeit zu gewährleisten und die Kontrolle und Souveränität über die eigenen Daten zu behalten.

Dieses Whitepaper fokussiert sich daher bewusst auf den rechtlichen Rahmen, insbesondere die Konformität mit der DSGVO, sowie auf Fragen zur Souveränität – und verzichtet auf einen Vergleich technischer Funktionen und Features. Die hier beschriebenen Lösungen Microsoft 365, eine klassisch betriebene Nextcloud und eine Managed Confidential Nextcloud auf Basis von Confidential Computing werden als funktional ausreichend für moderne Kollaboration angesehen.

Da Microsoft 365 keine vollwertige On-Premises-Lösung bietet, werden im Folgenden auch nur die SaaS-Angebote der beiden Nextcloud-Varianten betrachtet. Grundsätzlich bietet eine lokal betriebene Lösung, wie sie Nextcloud ermöglicht, noch einmal stärkeren Schutz, jedoch verbunden mit Abstrichen im Hinblick auf die Flexibilität von Cloud-Lösungen.

2 Microsoft 365: Bewertung aus DSGVO- und Souveränitätssicht

Microsoft 365 bietet einen breiten Funktionsumfang, ist jedoch aus Sicht des Datenschutzes und der Souveränität mit strukturellen Risiken verbunden. Zwar unterstützt Microsoft mit der EU-Data-Boundary die Datenresidenz innerhalb Europas. Doch als Unternehmen unterliegt es per Definition problematischen US-Gesetzen wie dem CLOUD Act. Dieser Grundkonflikt wurde im Juni 2025 deutlich: Der Chefjustiziar von Microsoft Frankreich bestätigte unter Eid, dass Microsoft nicht garantieren könne, dass Daten nicht an US-Behörden weitergegeben werden. Jenseits theoretischer Szenarien verdeutlicht auch der Fall des Chefanklägers des Internationalen Strafgerichtshofs, dessen Microsoft-Konto 2025 im Rahmen einer US-Sanktionsanordnung zeitweise gesperrt wurde, den realen Einfluss politischer Spannungen auf die digitale Infrastruktur – bis hin zum faktischen „Kill Switch" für zentrale Dienste.

Die Verarbeitung personenbezogener Daten durch ein US-Unternehmen bleibt also trotz vertraglicher und technischer Maßnahmen problematisch. Kritikpunkte betreffen auch die umfangreiche System- und Telemetriedaten-Erhebung, deren Umfang und Zweck weder vollständig transparent noch granular kontrollierbar sind. Ebenso gilt die Rollenverteilung zwischen Verantwortlichem und Auftragsverarbeiter seit Jahren als unklar, was eine DSGVO-konforme Nutzung erschwert. Das Gleiche gilt für in der DSGVO vorgeschriebenen Data Protection Impact Assessments (DPIA) und die seit Schrems-II erforderlichen Transfer Impact Assessments (TIA), die angesichts des CLOUD-Acts immer risikobehaftet ausfallen.

Auch in Bezug auf Datensouveränität besteht eine starke Abhängigkeit vom Anbieter. Weder Infrastruktur noch Kernkomponenten können eigenständig kontrolliert oder auditiert werden, und ein Wechsel auf alternative Plattformen ist aufgrund tief integrierter proprietärer Strukturen mit erheblichem Aufwand verbunden.

Insgesamt zeigt sich: Der breite Funktionsumfang von Microsoft 365 ist attraktiv. Doch mit Blick auf die DSGVO, die Auditierbarkeit und die langfristigen Souveränitätsziele bleibt ein nicht eliminierbares Restrisiko bestehen.

3 Nextcloud: DSGVO-konform dank EU-Hosting

Als europäische Alternative zu proprietären US-Plattformen ermöglicht eine in der EU betriebene Nextcloud eine nachweisbar DSGVO-konforme Verarbeitung ohne Datenübermittlungen in Drittländer. Unternehmen behalten so die vollständige Kontrolle über Speicherort, Verschlüsselung und Zugriffswege, und minimieren dadurch Risiken durch extraterritoriale Gesetze wie dem CLOUD Act.

Durch den vollständig offenen Quellcode lassen sich Sicherheitsaspekte, Datenverkehr und Konfigurationen unabhängig prüfen und dokumentieren. Diese Transparenz erleichtert Audits und reduziert Compliance-Unsicherheiten. Da Daten nicht in Drittländer transferiert werden, entfällt auch die Notwendigkeit für TIAs. DPIAs sind weiterhin notwendig – aber die Unternehmen können ihr Risiko selbst regulieren, indem sie zum Beispiel die Anzahl der Nutzer einschränken.

Da Nextcloud auf offenen Standards aufbaut, wird auch der sogenannte Vendor Lock-in vermieden. Organisationen wahren so ihre Unabhängigkeit bei der Wahl von Hosting, Infrastruktur und Sicherheitskonzept. Für Unternehmen wie für Behörden ist dieses Offenheitsprinzip ein zentraler Baustein digitaler, technischer und rechtlicher Souveränität.

DSGVO-konforme SaaS-Bereitstellung: Managed Nextcloud der HKN

Die Managed Nextcloud der HKN richtet sich an Organisationen, die eine souveräne Nextcloud nutzen möchten, ohne den sicherheitskritischen Plattformbetrieb selbst zu übernehmen. Die Bereitstellung erfolgt DSGVO-konform in deutschen Rechenzentren mit zertifizierten Prozessen nach ISO 9001 und ISO 27001. Sämtliche Daten und Backups verbleiben in Deutschland, werden verschlüsselt übertragen und in mandantenisolierten Umgebungen betrieben.

Jede Organisation erhält eine eigene Instanz mit vollen Administrationsrechten und damit direkte Kontrolle über Berechtigungen und Verschlüsselungsoptionen. HKN verzichtet auf Hyperscaler-Infrastrukturen und damit auf potenzielle Konflikte mit nicht-europäischen Rechtsordnungen. Inhalte und Metadaten werden grundsätzlich nicht an Dritte weitergegeben. Durch eine redundante Infrastruktur, tägliche Offsite-Backups und klar definierte Recovery-Prozesse wird zudem die Integrität und Verfügbarkeit der Daten abgesichert – ohne dass Unternehmen eigene Sicherheitsressourcen vorhalten müssen.

Eine klassische Nextcloud, auch in der Managed-Variante der HKN, erfüllt die Anforderungen der DSGVO in Bezug auf Datenresidenz, verfügt über eine zertifizierte Infrastruktur und bietet Nutzern verschiedene Optionen, den Zugriff auf ihre Daten effektiv zu kontrollieren. Eine Steigerung in Sachen Sicherheit und Vertraulichkeit bietet dabei die Möglichkeit, die Managed Nextcloud mittels Confidential Computing durchgängig zu verschlüsseln.

Über HKN

Die HKN GmbH ist ein Spezialist für Open-Source-basierte Cloud-Lösungen mit höchsten Sicherheits- und Datenschutzstandards. Seit 1996 betreibt HKN eine eigene Rechenzentrumsinfrastruktur in Deutschland und entwickelt digitale Arbeitsplätze für Unternehmen und öffentliche Auftraggeber – souverän, DSGVO-konform und unabhängig von US-Anbietern.

4 Managed Confidential Nextcloud: Souveränität durch Confidential Computing

Die Managed Confidential Nextcloud erweitert das Sicherheitsmodell der klassischen Nextcloud um eine zusätzliche technische Schutzebene: Confidential Computing. Während Daten bisher nur im Ruhezustand und bei der Übertragung verschlüsselt werden konnten, schützt Confidential Computing diese nun auch während der Verarbeitung („3D-Verschlüsselung“).

Nextcloud-Workloads werden dabei in hardwarebasierten Trusted Execution Environments (TEEs) – sogenannten Enklaven – ausgeführt, deren Integrität durch kryptografische Attestation nachweisbar ist. Diese isolierten Ausführungsumgebungen werden durch das deutsche Unternehmen enclaive bereitgestellt und stellen sicher, dass selbst privilegierte Administratoren keine Einsicht in Klartextdaten erhalten. Weder HKN als Betreiber der Nextcloud noch enclaive oder sonstige Dritte können auf die Inhalte innerhalb dieser abgeschotteten Umgebung zugreifen.

In Bezug auf die DSGVO und digitale Souveränität bedeutet dieses Zero-Access-Modell eine erhebliche Reduktion technischer Risiken und bietet die stärkste Form der Kontrolle: Die Schlüsselhoheit verbleibt vollständig beim Kunden (Hold Your Own Key), während die gesamte Datenverarbeitung in den zertifizierten deutschen Rechenzentren der HKN stattfindet. Offene Standards, vollständige Auditierbarkeit und eine starke Datenisolation in allen Dimensionen tragen ebenso entscheidend zur nachweisbaren Selbstbestimmtheit bei. Die Enklaven von enclaive verfügen dabei bereits über Post-Quanten-sichere Verschlüsselung, sind also auch langfristig sicher vor Zugriffen staatlicher Akteure oder Cyberkrimineller.

Für Sektoren mit hochsensiblen Daten wie dem Gesundheitswesen, der öffentlichen Verwaltung, der Finanzbranche oder Industrie und Forschung ist die Confidential Nextcloud damit ein robustes Fundament für eine europäisch kontrollierte Kollaborationsplattform.

Über enclaive

enclaive ist ein Unternehmen mit Hauptsitz in Berlin und spezialisiert auf Confidential Computing, einen neuartigen Security-Ansatz, der Daten erstmals in allen drei Dimensionen (**at rest**, **in transit**, **in use**) verschlüsselt. enclaive verfolgt dabei einen ganzheitlichen Security-Ansatz: Über die enclaive Multi-Cloud-Plattform lassen sich Post-Quanten-sichere Virtual Machines, Kubernetes-Cluster und Databases einrichten. Die Enklaven lassen sich ohne Code-Änderungen in bestehende Infrastruktur integrieren und verursachen kaum zusätzlichen Rechenaufwand. enclaive bietet mit seinem virtuellen HSM zudem die nötigen Trust Elemente wie Key Management und Workload Identity Management & Attestation Service als eigenständige Produkte. Und mit Garnet, einer GenAI-Firewall, steht ein starker Schutzschild zur Daten-sicheren Nutzung von externen KI-Tools bereit.

Fazit

Alle hier verglichenen Lösungen bieten praktische Funktionen für eine zeitgemäße Zusammenarbeit, unterscheiden sich jedoch deutlich in Bezug auf Datenschutz und Souveränität. Microsoft 365 bleibt aufgrund der unsicheren internationalen Rechtslage und der begrenzten Kontrollmöglichkeiten ein strategisches Risiko. Eine klassische Nextcloud bietet ein hohes Maß an Compliance und Transparenz und ist damit für viele Organisationen eine sichere Wahl.

Für besonders sensible Daten, strenge regulatorische Anforderungen oder Branchen mit erhöhtem Schutzbedarf bietet die Managed Confidential Nextcloud ein Höchstmaß an Datensouveränität und technischen Schutzmechanismen. Sie vereint europäische Datenhaltung, offene Technologien und Confidential Computing in einer durchgängigen Plattform und sichert so maximale Kontrolle und Datenschutz auf höchstem Niveau.

Kriterium	Microsoft 365	Klassische Nextcloud	Managed Confidential Nextcloud
DSGVO-Konformität	Strukturell problematisch (CLOUD Act); Compliance bleibt risikobehaftet (Schrems II, TIA/DPIA).	DSGVO-konform durch Hosting in Deutschland/EU; TIAs entfallen, DPIA mit kontrollierbarem Risiko	DSGVO-konform durch Hosting in Deutschland/EU; TIAs entfallen, DPIA positiv dank Zero-Access-Modell.
Datenresidenz	EU-Data-Boundary, jedoch kein Schutz vor extraterritorialen Zugriffen.	Deutschland/EU	Deutschland/EU
Datenzugriff durch Dritte	Potenzieller Zugriff durch US-Behörden; Telemetrie- und Systemdaten wenig transparent.	Kein struktureller Fremdzugriff; HKN-Administratoren haben im Notfall Zugriff	Kein Zugriff möglich (auch nicht durch HKN oder enclaive); TEEs verhindern Einsicht in Klartextdaten
Verschlüsselung	At Rest + In Transit	At Rest + In Transit	At Rest, In Transit, In Use in isolierten TEEs
Transparenz & Auditierbarkeit	Gering (Proprietäre Plattform)	Hoch (Open Source); HKN zertifiziert nach ISO 9001 und 27001	Sehr hoch: Wie klassische Nextcloud, zusätzlich nachweisbare Integrität der Enklaven (Attestation)

Kriterium	Microsoft 365	Klassische Nextcloud	Managed Confidential Nextcloud
Souveränität	Gering; Zugriffe durch US-Behörden + hoher Vendor Lock-in durch proprietäres Ökosystem und enge Integration.	Hoch; Offene Standards, Open Source, freie Wahl von Hosting & Integrationen	Sehr hoch; wie klassische Nextcloud + Schlüsselhoheit (Hold Your Own Key)
Geeignet für hochsensible Daten	Nein	Begrenzt	Ja