[abtis]
DIGITALE ZUKUNFT

SOUVERÄN. SICHER. SKALIERBAR.

Digitale Souveränität und Resilienz
für eine sichere Zukunft im Mittelstand.

Microsoft
DIGITAL RESILIENCE
PARTNER OF THE YEAR
2025
Microsoft
Digital Resilience Partner of the Year
2025

SOUVERÄNE CLOUD

Souveränität als Schlüssel zur digitalen Zukunft

In a nutshell

Die Digitalisierung ist zum Fundament des wirtschaftlichen Erfolgs geworden – doch mit wachsender Vernetzung steigt auch die Abhängigkeit von globalen Plattformen, außereuropäischen Gesetzen und komplexen Compliance-Vorgaben. Für den deutschen Mittelstand und die öffentliche Hand bedeutet das: Innovation braucht Vertrauen, Sicherheit und Kontrolle über Daten, Prozesse und Infrastruktur.

Warum jetzt handeln?

Über 80 % der europäischen Cloud-Infrastruktur liegt in der Hand außereuropäischer Anbieter. Gleichzeitig verschärfen Gesetze wie DSGVO, NIS2 und DORA die Anforderungen an Datenschutz, IT-Sicherheit und Governance. Wer diese Herausforderungen ignoriert, riskiert nicht nur Bußgelder, sondern auch Wettbewerbsfähigkeit und digitale Handlungsfreiheit.

Der abtis Weg zur souveränen Cloud

Gemeinsam mit Microsoft bietet abtis einen abgestuften Ansatz für digitale Souveränität – das Sovereignty Spectrum. Von der Sovereign Public Cloud über Azure Local bis zur Delos Cloud verbindet es globale Innovation mit nationaler Verantwortung. Organisationen behalten die Hoheit über ihre Daten und Schlüssel, sichern Compliance nach europäischen Standards und profitieren gleichzeitig von der vollen Leistungsfähigkeit moderner Cloud-Technologien.

Das Ergebnis: Vertrauen, Kontrolle und Zukunftssicherheit

Die souveräne Cloud schafft den Spagat zwischen Innovation und Sicherheit. Sie stärkt die digitale Resilienz, reduziert Abhängigkeiten und ermöglicht nachhaltiges Wachstum – souverän, sicher und skalierbar.

Dynamik des Fortschritts

Digitalisierung als Erfolgsfaktor im Mittelstand

Cloud als Rückgrat des digitalen Mittelstands: Die Cloud ist längst kein Innovationsprojekt mehr. Sie ist zur unverzichtbaren Basis-Infrastruktur der deutschen Wirtschaft geworden. Laut Bitkom Cloud Report 2025 setzen heute 90 % der deutschen Unternehmen Cloud-Lösungen ein, ein signifikanter Anstieg gegenüber 81 % im Vorjahr. 62 % geben an, dass ohne Cloud-Dienste zentrale Geschäftsprozesse stillstehen würden. Damit ist die Cloud nicht nur eine Technologiefrage, sondern ein kritischer Wettbewerbsfaktor für Unternehmen in allen Branchen.

Der Mittelstand im Umbruch: Für den deutschen Mittelstand - Rückgrat der Volkswirtschaft mit über 3,5 Millionen Unternehmen - ist Cloud-Technologie ein Schlüssel zur Zukunftsfähigkeit. Angesichts von Fachkräftemangel, steigendem Innovationsdruck und globalem Wettbewerbsdruck bietet die Cloud dringend benötigte Flexibilität, Skalierbarkeit und Zugang zu neuen Technologien. Besonders relevant: Cloud-Services ermöglichen es mittelständischen Unternehmen, KI, Automatisierung und moderne Sicherheitslösungen auch ohne große interne IT-Teams zu nutzen.

Regulierter Sektor: Auch in regulierten Branchen wie Finanzen, Energie, Gesundheitswesen und dem öffentlichen Sektor steigt die Nachfrage nach vertrauenswürdigen Cloud-Lösungen. Hier steht nicht nur Effizienz, sondern Compliance, Datenschutz und Kontrollierbarkeit im Vordergrund. Anbieter wie Microsoft investieren gezielt in lokal konforme Infrastrukturen - beispielsweise mit Azure-Regionen in Deutschland und Angeboten wie Microsoft 365 Local oder Delos Cloud.

Cloud-Investitionen nehmen weiter Fahrt auf: Über 50 % der Unternehmen planen, ihre Cloud-Nutzung in den kommenden Jahren auszubauen. Aktuell werden bereits 47 % aller IT-Anwendungen aus der Cloud betrieben - bis 2030 soll dieser Anteil auf über 58 % steigen. Parallel dazu baut Microsoft seine Cloud-Kapazitäten in Deutschland massiv aus. Die Botschaft ist klar: Wer digital wettbewerbsfähig bleiben will, muss die Cloud strategisch nutzen - und zwar jetzt.

90% Cloud-Nutzung

Fast alle deutschen Unternehmen nutzen die Cloud

62% Abhängigkeit

Unternehmen sind auf die Cloud angewiesen

58% Cloud-Anteil

Anteil der Cloud-Anwendungen steigt bis 2030

Compliance nachhaltig sicherstellen

Zunehmende regulatorische Anforderungen

Compliance wird zur Pflicht: Mit der DSGVO hat die EU bereits 2018 hohe Datenschutzstandards gesetzt. Für Cloud-Nutzer bedeutet das: Datenverarbeitung durch Dritte – also auch Cloud-Anbieter – gilt als Auftragsverarbeitung und unterliegt strenger Kontrolle. Unternehmen sind verpflichtet, ihre Anbieter sorgfältig zu prüfen und klare Vereinbarungen zur Datenhoheit zu treffen.

NIS2 - Cybersecurity auf Vorstandsebene: Die NIS2-Richtlinie, deren Umsetzung in Deutschland für Ende 2025 erwartet wird, betrifft über 30.000 Unternehmen. Sie verpflichtet Organisationen u. a. zu Risikomanagement, Vorfallmeldungen, Backup-Konzepten und Absicherung der Lieferkette. Bei Verstößen drohen Bußgelder von bis zu 20 Mio. € oder 4 % des Umsatzes – Cybersecurity wird damit zur Chefsache.

DORA - Neue Maßstäbe für den Finanzsektor: Der Digital Operational Resilience Act (DORA) gilt seit Januar 2025 und reguliert die digitale Resilienz im EU-Finanzsektor. Über 22.000 Finanzinstitute und ihre IT-Dienstleister sind verpflichtet, IT-Risiken zu managen, Stresstests durchzuführen und IKT-Drittparteien strikt zu überwachen. Auch Cloud-Provider rücken stärker in den Fokus der Aufsicht.

CRA & EU Data Act: Der Cyber Resilience Act (CRA) setzt ab 2027 neue Standards für die IT-Sicherheit von Software und digitalen Produkten – inklusive Meldepflichten, Updates und Nachweispflichten. Gleichzeitig verpflichtet der EU Data Act Cloud-Anbieter dazu, Wechselbarrieren abzubauen und Datenportabilität zu gewährleisten, was direkte Auswirkungen auf Vertragsmodelle und Plattformarchitekturen hat.

Regulatorik als Innovationsmotor: Ob Mittelstand oder Großunternehmen – die Verdichtung regulatorischer Anforderungen zwingt Organisationen zum Umdenken. Souveräne Cloud-Lösungen helfen, Compliance nachhaltig sicherzustellen und schaffen gleichzeitig Vertrauen bei Kunden, Partnern und Aufsichtsbehörden.

Geopolitische Unsicherheiten

Abhängigkeiten von außereuropäischen Anbietern

Technologische Abhängigkeit als strategisches Risiko: Europa ist digital stark abhängig von außereuropäischen Cloud-Anbietern – insbesondere aus den USA. Über 80 % des europäischen Cloud-Markts werden von US-Hyperscalern kontrolliert, allen voran Amazon Web Services (AWS) mit 53 % Marktanteil in Europa. Diese Konzentration schafft nicht nur wirtschaftliche, sondern auch politische Risiken. 78 % der deutschen Unternehmen halten die Abhängigkeit von US-Clouds für zu hoch, und 82 % wünschen sich europäische Alternativen.

Rechtliche und politische Unsicherheiten: Der US CLOUD Act von 2018 erlaubt US-Behörden, auf Daten von US-Cloud-Anbietern zuzugreifen – selbst wenn diese physisch in europäischen Rechenzentren liegen. Damit entsteht ein direkter Konflikt mit der DSGVO und europäischen Datenschutzprinzipien. Das Schrems-II-Urteil des Europäischen Gerichtshofs von 2020 hat diese Unsicherheit noch verstärkt: Der Wegfall des Privacy Shield zwingt Unternehmen seither zu individuellen Risikoanalysen, technischen Schutzmaßnahmen und aufwendiger Dokumentation.

Geopolitische Spannungen als Cloud-Risiko: Der technologische Systemwettbewerb zwischen den USA und China verschiebt die globale Machtbalance. Technologie wird zunehmend zur geopolitischen Waffe – und Daten zum strategischen Gut. Für deutsche Unternehmen rückt daher das „vertrauenswürdige Herkunftsland“ als Kriterium für Cloud-Anbieter in den Fokus: 67 % betrachten es inzwischen als zwingend, gegenüber 58 % im Vorjahr. Diese Entwicklung unterstreicht den Wunsch nach digitaler Souveränität und rechtlicher Sicherheit.

Das Risiko wächst: Ein politischer Konflikt, eine Sanktion oder ein Provider-Stopp könnte ganze Geschäftsprozesse lahmlegen. Experten warnen, dass einzelne Anbieter mit einem Knopfdruck kritische Systeme abschalten könnten. Laut Gartner werden daher bis 2030 über 75 % der europäischen Unternehmen ihre Workloads in souveräne oder geopolitisch resiliente Cloud-Umgebungen verlagern. Technologische Unabhängigkeit wird zum zentralen Bestandteil wirtschaftlicher Sicherheit.

80% Cloud-Markt

werden von US-Hyperscalern kontrolliert

US CLOUD Act

erlaubt US-Behörden, auf Cloud zuzugreifen

67% Herkunftsland

sehen das als Kriterium für Cloud-Anbieter

Neue souveräne Lösungen

Microsofts "European Digital Commitments" als Grundlage für digitale Resilienz

Europäische Infrastruktur ausbauen: Mit den European Digital Commitments reagiert Microsoft auf Europas wachsenden Bedarf an Datenschutz, Kontrolle und digitaler Unabhängigkeit. Bis 2027 wächst das europäische Rechenzentrumsnetz auf über 200 Standorte – ein Plus von 40 %. Ergänzend verpflichtet sich Microsoft mit dem Digital Resilience Promise, behördliche Eingriffe oder Aussetzungsanordnungen in europäischen Cloud-Operationen konsequent anzufechten und damit die digitale Handlungsfähigkeit europäischer Organisationen zu schützen.

Datenschutz nach EU-Standards: Die vollständig abgeschlossene EU Data Boundary garantiert, dass Kundendaten für Microsoft 365, Dynamics 365, Azure und Azure AI ausschließlich innerhalb Europas verarbeitet werden – einschließlich technischer Telemetrie und KI-bezogener Datenflüsse. Gleichzeitig investiert Microsoft in europäische Cybersecurity-Partnerschaften, stärkt die Zusammenarbeit mit Behörden und fördert offene Standards und Wettbewerbsfähigkeit im europäischen Cloud-Ökosystem.

Bausteine souveräner Cloud-Technologie

Unter dem Dach der Microsoft Sovereign Cloud bündelt Microsoft die zentralen Technologien für souveränitätskritische Organisationen:

- Data Guardian überwacht und protokolliert Zugriffe, die ausschließlich durch autorisiertes EU-Personal erfolgen dürfen.
- External Key Management gibt Kunden die vollständige Kontrolle über ihre Verschlüsselungsschlüssel – gespeichert in eigenen oder zertifizierten HSMs.
- Regulated Environment Management zentralisiert alle Souveränitätsfunktionen, Richtlinien und Compliance-Nachweise und macht Vorgaben revisionssicher überprüfbar. Ergänzt wird dies durch Microsoft 365 Local und Azure Local, die Cloud-Dienste in vollständig kontrollierten und auf Wunsch isolierten Umgebungen bereitstellen.

Nationales Vorbild: Die Delos Cloud in Deutschland zeigt, wie globale Innovation und nationale Hoheit vereint werden können: betrieben unter deutscher Kontrolle, basierend auf Azure-Technologie und vollständig konform mit BSI- und IT-Grundschutzvorgaben. Sie gilt als Referenzmodell dafür, wie resiliente, rechtssichere und souveräne Cloud-Strukturen in Europa aufgebaut werden können – von der Bundesverwaltung bis hin zu KRITIS-Betreibern.

Relevanz von digitaler Souveränität

Datensouveränität, operative und technologische Souveränität

Die drei Dimensionen digitaler Souveränität gehören heute zu den entscheidenden Leitplanken einer sicheren und zukunftsfähigen Cloud-Strategie. Laut Gartner entsteht belastbare digitale Souveränität erst durch das Zusammenspiel von Kontrolle, Transparenz und Unabhängigkeit – und schützt Unternehmen damit vor rechtlichen, technischen und geopolitischen Risiken, die in einer global vernetzten IT-Landschaft stetig zunehmen.

- Datensouveränität – Kontrolle über Speicherort, Zugriff und Verschlüsselung sensibler Informationen.
- Operative Souveränität – Hoheit über Betriebsprozesse, Support-Strukturen und Incident Management – auch im Cloud-Betrieb.
- Technologische Souveränität – Unabhängigkeit durch offene Standards, portable Workloads und den Einsatz von Open Source.

Strategischer Erfolgsfaktor: Gartner erwartet, dass bis Ende 2025 rund 30 % der Unternehmen wirtschaftliche oder rechtliche Schäden erleiden werden, wenn sie digitale Abhängigkeiten nicht aktiv steuern. Organisationen, die frühzeitig auf souveräne Architekturen setzen, stärken ihre Resilienz, erhöhen das Vertrauen von Kunden und Partnern und sichern langfristig ihre Innovations- und Investitionsfähigkeit – besonders in einer Zeit, in der Regulierung und Cyberrisiken weiter ansteigen.

Der europäische Weg: Europa setzt verstärkt auf vertrauenswürdige Infrastrukturen, offene Technologien und föderierte Cloud-Modelle. Initiativen wie die deutsch-französische Open-Source-Kooperation openDesk oder die Programme der EU-Digitalen Dekade zeigen, wie Interoperabilität, Datenschutz und moderne Cloud-Technologie miteinander verzahnt werden können und gleichzeitig europäische Werte gestärkt werden. Für Unternehmen bedeutet das: kritische Daten bewusst in europäischen Regionen betreiben, zertifizierte Partner wählen und Cloud-Architekturen einsetzen, die Portabilität, Governance und Compliance von Anfang an berücksichtigen – als Basis für nachhaltige digitale Souveränität.

Digitale Souveränität entsteht durch das Zusammenspiel von Kontrolle, Transparenz und Unabhängigkeit. Unternehmen, die diese Dimensionen früh verankern, schützen sich wirksam vor rechtlichen, technischen und geopolitischen Risiken und schaffen die Basis für belastbare digitale Infrastrukturen. Souveräne Architekturen ermöglichen es, sensible Daten gezielt zu steuern, Prozesse nachvollziehbar zu halten und Abhängigkeiten zu reduzieren.

Digitale Angriffsflächen erkennen

Viele Organisationen blockieren Cloud-Lösungen aus Compliance-Bedenken

Compliance als Umsetzungsbremse:

Trotz breiter Cloud-Nutzung herrscht vielerorts Zurückhaltung. Unternehmen sehen sich mit steigenden Anforderungen aus der DSGVO, NIS2, DORA und dem CRA konfrontiert. Die Angst vor Fehlkonfigurationen, Datenverlust oder Kontrollverlust führt dazu, dass Cloud-Projekte aufgeschoben oder gestoppt werden – insbesondere in regulierten Branchen und bei sensiblen Workloads.

Regulatorische Komplexität und interne Hürden:

Je nach Sektor gelten unterschiedliche Vorgaben: Finanz- und Gesundheitswesen benötigen zusätzliche Nachweise (z. B. BSI C5), Behörden setzen auf IT-Grundschutz. Parallel erschwert der Betriebsrat in vielen Fällen die Einführung cloudbasierter Anwendungen – etwa bei Microsoft 365 – aufgrund von Mitbestimmungsrechten bei IT-Systemen mit Überwachungspotenzial.

Fehlendes Know-how und Change Management:

Cloud-Migration erfordert neue Kompetenzen im Bereich Governance, Security und Betriebsmodell. Ohne gezielte Weiterbildung entstehen Unsicherheiten, die Projekte blockieren. Auch fehlende Abstimmung zwischen IT, Datenschutz, Recht und Management verzögert Entscheidungen und erhöht die Komplexität.

Mythen und Missverständnisse:

Noch immer halten sich Annahmen wie „Cloud = Kontrollverlust“ oder „On-Premises ist sicherer“. Dabei gelten für die Cloud das Shared Responsibility Model und höchste Standards bei Verschlüsselung, Zugriffskontrolle und Redundanz. Hyperscaler investieren Milliarden in ihre Sicherheitsarchitekturen – oft deutlich mehr als einzelne Unternehmen leisten könnten.

Vertrauen braucht Transparenz: Organisationen müssen ihre Cloud-Strategie regulatorisch fundieren, technisch absichern und organisatorisch begleiten. Wer Governance, Verschlüsselung und Datensouveränität von Anfang an mitdenkt, kann moderne Cloud-Lösungen nutzen – compliant, sicher und innovationsfähig.

Herausforderungen im Mittelstand

Fehlendes Vertrauen in Datenverarbeitung außerhalb Europas

Datenschutzkonflikte als Vertrauensbarriere: Viele Organisationen zögern beim Einsatz internationaler Cloud-Anbieter – aus gutem Grund: Der US CLOUD Act erlaubt Behörden Zugriff auf Daten von US-Unternehmen, selbst wenn diese physisch in Europa liegen. Das kollidiert mit der DSGVO und schafft Rechtsunsicherheit. Spätestens seit dem Schrems-II-Urteil des EuGH ist klar: Der Schutz personenbezogener Daten außerhalb der EU ist nicht gewährleistet – Unternehmen müssen jeden Einzelfall prüfen und technisch absichern.

Souveränität wird zum Auswahlkriterium: Die Folgen sind deutlich messbar: 78 % der deutschen Unternehmen halten die Abhängigkeit von US-Clouds für zu hoch, 82 % wünschen sich europäische Alternativen. Für 67 % ist ein vertrauenswürdiges Herkunftsland inzwischen zwingende Voraussetzung bei der Anbieterwahl – alle Befragten bevorzugen Anbieter aus Deutschland. Das Herkunftsland wird zum Sicherheitsfaktor.

Vertrauen durch Zertifizierung und Transparenz: Zertifikate wie ISO 27018, BSI C5 oder der EU Cloud Code of Conduct schaffen belastbare Nachweise für Datenschutz, Sicherheit und DSGVO-Konformität. Sie werden insbesondere im Mittelstand und in regulierten Branchen zum Mindeststandard. Auch Initiativen wie Gaia-X stärken das Vertrauen: Sie setzen auf Open-Source, Dezentralität und Interoperabilität – basierend auf europäischen Werten.

Europäische Lösungen gewinnen an Relevanz: Nationale Modelle wie Delos Cloud oder Bleu (Frankreich) zeigen, dass sich leistungsfähige Cloud-Technologie und europäische Rechtsstandards kombinieren lassen. Microsoft unterstützt diese Entwicklung aktiv mit der EU Data Boundary, External Key Management und Data Guardian – für volle Kontrolle über Speicherort, Zugriff und Verschlüsselung.

Transparenz als Erfolgsfaktor im Betrieb: Viele Unternehmen berichten, dass fehlende Einblicke in Betriebsprozesse, Supportstrukturen und Incident-Handling internationaler Anbieter das Vertrauen zusätzlich belasten. Souveräne Cloud-Lösungen schaffen hier Abhilfe durch klare Verantwortlichkeiten, nachvollziehbare Betriebsmodelle und überprüfbare Zugriffskontrollen – ein entscheidender Baustein für nachhaltige Cloud-Akzeptanz.

Souveräne Cloud-Modelle gewinnen an Bedeutung, weil sie ein Kernproblem lösen: fehlendes Vertrauen in internationale Datenverarbeitung. Rechtssicherheit, transparente Betriebsmodelle und überprüfbare Zugriffskontrollen bilden die Basis belastbarer Cloud-Strategien. Europäische Lösungen zeigen mit modernen Souveränitätstechnologien, dass Datenschutz, Compliance und Innovation verlässliche digitale Transformation ermöglichen.

Herausforderungen im Mittelstand

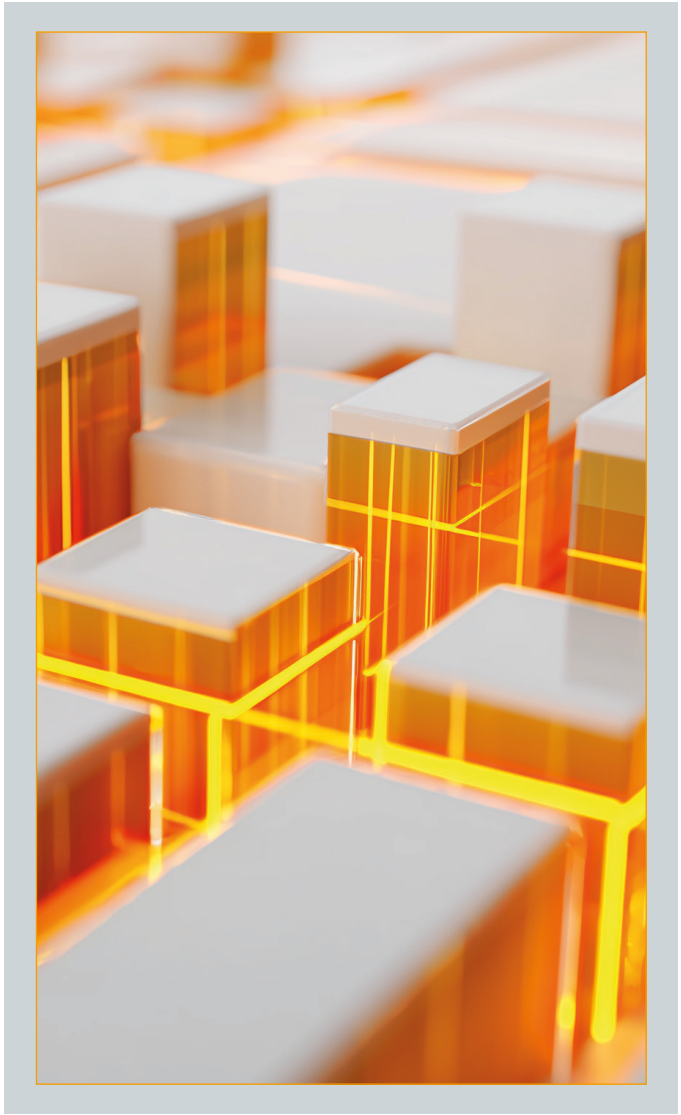
Bedarf nach Sicherheit, Kontrolle und Transparenz

Souveränität bei vollem Funktionsumfang: Der Wunsch nach Innovationskraft kollidiert für viele Unternehmen noch immer mit Anforderungen an Datenschutz, Kontrolle und rechtlicher Sicherheit. Moderne Cloud-Technologien zeigen jedoch: Beides lässt sich vereinen. Funktionen wie Microsofts Data Guardian, External Key Management und Confidential Computing ermöglichen die Nutzung leistungsfähiger Cloud-Dienste bei gleichzeitig strikter Einhaltung regulatorischer Vorgaben – ohne Kompromisse bei Funktionsumfang, Performance oder Skalierbarkeit. Damit wird Souveränität nicht zur Bremse, sondern zum Gestaltungsraum für sichere digitale Transformation.

Sicherheit als Innovationsbeschleuniger: Technische Schutzmaßnahmen wie verschlüsselte Trusted Execution Environments, kontrollierter Schlüsselzugriff und DSGVO-konforme Datenhaltung schaffen Vertrauen und bilden die Grundlage für den Einsatz moderner KI- und Automatisierungslösungen. KI-gestützte Cloud-Umgebungen steigern Effizienz deutlich – durch optimierte Workload-Steuerung, automatisierte Sicherheitsmechanismen und kontinuierliches Security Monitoring. Für mittelständische Unternehmen entsteht so ein Sicherheitsniveau, das interne Teams allein kaum realisieren könnten.

Transparente Governance schafft Handlungsspielraum: Mit zertifizierten Partnern, klaren Betriebsmodellen und überprüfbaren Sicherheitsprozessen lassen sich selbst sensible Workloads rechtskonform in die Cloud überführen. Die Einhaltung von Standards wie ISO 27018, BSI C5 oder dem EU Cloud Code of Conduct wird zum strategischen Vorteil: Sie schafft Klarheit, reduziert Audit-Aufwände und sorgt dafür, dass Governance nicht als Hindernis wahrgenommen wird, sondern als Enabler für eine stabile und kontrollierbare Cloud-Infrastruktur.

Wer Governance und Transparenz früh verankert, nutzt Cloud-Plattformen souverän und sicher – auch in regulierten Umgebungen. Geprüfte Sicherheit und klare Verantwortlichkeiten bringen nicht nur Rechtskonformität, sondern auch Skalierbarkeit und Innovationskraft.



Herausforderungen im Mittelstand

Unterschiedliche regulatorische Ansprüche: Mittelstand vs. öffentlicher Sektor

Einheitliche Technologie, unterschiedliche Spielregeln: Cloud-Nutzung erfolgt unter sehr unterschiedlichen regulatorischen Rahmenbedingungen. Während der Mittelstand vor allem Effizienz, Skalierbarkeit und schnellen Innovationszugang sucht, steht im öffentlichen Sektor der rechtssichere und vollständig nachvollziehbare Betrieb im Vordergrund. Je nach Branche und Unternehmensgröße greifen unterschiedliche Pflichten – von DSGVO und NIS2 über DORA bis zum BSI IT-Grundschutz. Das erzeugt ein komplexes Spannungsfeld, das ohne klare Governance-Modelle und definierte Verantwortlichkeiten schwer beherrschbar ist.

Mittelstand zwischen Aufbruch und Unsicherheit: Viele mittelständische Unternehmen wünschen sich mehr digitale Freiheit, stoßen jedoch auf organisatorische und rechtliche Hürden. Mitbestimmung durch den Betriebsrat, Fachkräftemangel sowie unklare Zertifizierungs- und Dokumentationspflichten bremsen Cloud-Initiativen spürbar aus. Gleichzeitig steigen die Erwartungen an Datenschutz, Verfügbarkeit und IT-Sicherheit – häufig ohne ausreichend interne Compliance-Expertise. Das führt zu Unsicherheit und verzögert Entscheidungen, obwohl die technische Notwendigkeit längst erkannt ist.

Verwaltungen brauchen höchste Konformität: Im öffentlichen Sektor gelten besonders strenge Maßstäbe. Cloud-Lösungen müssen durchgängig mit IT-Grundschutz, Geheimhaltungsanforderungen und Vorgaben wie § 5 BSI-KritisV harmonieren. Externe Dienste sind oft nur bei klar belegbarer Rechtslage zulässig. Entsprechend hoch ist die Nachfrage nach vollständig souveränen Betriebsmodellen – technisch wie organisatorisch –, bei denen Daten, Schlüssel und Betrieb verlässlich unter nationaler Kontrolle stehen.

Zertifizierungen als Schlüssel zur Vertrauensbildung: Standards wie BSI C5, ISO 27018 oder der EU Cloud Code of Conduct gewinnen deutlich an Bedeutung. Sie schaffen Transparenz, Rechtssicherheit und verbindliche Mindestanforderungen. Im Mittelstand dienen sie als Orientierungshilfe, in der Verwaltung häufig als zwingende Voraussetzung. Anbieter, die solche Nachweise erfüllen und moderne Governance-Mechanismen wie Policy-as-Code unterstützen, ermöglichen einen souveränen und konformen Cloud-Betrieb über alle Compliance-Stufen hinweg.

Cloud-Strategien brauchen regulatorische Passung. Der Weg in die Cloud ist kein Standardprozess. Organisationen müssen ihre Anforderungen sektorenspezifisch bewerten – und Lösungen wählen, die technische Leistungsfähigkeit und regulatorische Konformität verbinden. Nur so gelingt die Balance zwischen Innovation und Sicherheit – im Mittelstand wie im Staat.

Stolpersteine in der Praxis

Datenlokalisierung, Schlüsselmanagement, Governance

Technische Komplexität trifft auf organisatorische Reibung: Viele Cloud-Projekte scheitern weniger an der Technologie als an fehlender Vorbereitung. Unklare Zuständigkeiten, fehlende Exit-Strategien oder unterschätzter Migrationsaufwand führen zu Verzögerungen und Sicherheitslücken. Oft fehlen ein durchdachtes Architektur- und Compliance-Design sowie verbindliche Betriebsmodelle. Gleichzeitig hält sich der Irrglaube, Sicherheit ließe sich vollständig an den Anbieter delegieren – ein Fehler, der operative Resilienz nachhaltig schwächen kann.

Datenlokalisierung – rechtlich gefordert, operativ anspruchsvoll: Die Verarbeitung sensibler Daten innerhalb definierter geografischer Grenzen ist in vielen Branchen Pflicht. Dafür braucht es saubere Datenklassifikation, passende Cloud-Zonen, klares Monitoring und Regeln für Workload-Platzierung. Fehler können regulatorische Verstöße und Verfügbarkeitsprobleme nach sich ziehen. Mit EU-Regelwerken wie Data Governance Act und Data Act steigen die Anforderungen weiter – Datenlokalisierung wird zum dauerhaften Steuerungsthema.

Schlüsselmanagement als Kontrollfrage: Ohne Hoheit über eigene Verschlüsselungsschlüssel verlieren Organisationen zentrale Kontrolle – mit Risiken für Compliance und Vertrauen. Der sichere Betrieb von HSMs oder External Key Management erfordert klare Prozesse, auditierbare Key-Rotation und eindeutige Verantwortlichkeiten. Moderne Methoden wie Confidential Computing schützen zusätzlich die Verarbeitung selbst und machen Schlüsselmanagement zur strategischen Leitplanke souveräner Cloud-Nutzung.

Governance – oft vernachlässigt, selten nachholbar: Transparente Prozesse, dokumentierte Verantwortlichkeiten und regelmäßige Compliance-Prüfungen sind Grundvoraussetzungen souveräner Cloud-Nutzung. Fehlen sie, entstehen blinde Flecken: Wer darf was? Wie werden Änderungen dokumentiert? Wie läuft Incident Response? Ohne konsistente Governance und Policy-as-Code wächst die Komplexität schneller als die Kontrolle. Souveräne Architekturen zeigen dagegen, wie standardisierte Kontrollen und revisionssichere Prozesse Governance zum Beschleuniger machen.

Wer souverän migrieren will, braucht Weitblick: Die größten Risiken liegen nicht in der Cloud selbst – sondern in ihrer Einführung. Unternehmen, die frühzeitig auf Klarheit, Struktur und Sicherheit setzen, schaffen die Grundlage für nachhaltigen Erfolg. Best Practices aus Europa zeigen: Souveräne Cloud ist möglich – mit dem richtigen Partner, der richtigen Strategie und dem Blick für das Ganze.

Wirksamer Schutz für Ihr Unternehmen

abtis Sovereignty Spectrum

Mit dem Sovereignty Spectrum bietet abtis einen klar strukturierten Weg zu digitaler Souveränität – abgestuft nach Bedarf, Risiko und Regulierung, ohne auf Innovation zu verzichten. Gemeinsam bilden die drei Stufen ein flexibles Spektrum für alle Souveränitätsgrade:

Souverän in der Public Cloud

Sovereign Public Cloud (Azure)

- EU Data Boundary & volle Datenresidenz in Europa
- Kontrolle über Zugriffe & Schlüssel (EKM, Data Guardian)
- Keine Migration notwendig – volle Azure-Funktionalität
- Ideal für Mittelstand & regulierte Branchen
- Schnell, skalierbar, compliant

Maximale Betriebshoheit mit Azure Local

Sovereign Private Cloud (Azure Local)

- Microsoft-Dienste auf zertifizierter Hardware „Made in Germany“
- Betrieb im eigenen oder staatlichen Rechenzentrum
- Optional vollständig isolierte / air-gapped Umgebungen
- Höchste Sicherheits- und Verfügbarkeitsstufen (KRITIS, Behörden)
- Lokaler Betrieb, hybride Flexibilität

Volle Souveränität unter nationaler Hoheit

National Partner Cloud (Delos Cloud)

- Cloud-Betrieb komplett in Deutschland, unabhängig von ausländischem Recht
- BSI C5, IT-Grundschutz & zukünftige VS-NfD-Fähigkeit
- Getrennte Betriebs-, Support- & Schlüsselhoheit
- Für Verwaltung & KRITIS mit höchsten Vertrauensanforderungen
- Microsoft-Technologie, national betrieben

Ihr Sicherheitsfundament

Stufe 1: Sovereign Public Cloud (Azure)

Grundidee: Die Sovereign Public Cloud ist der einfachste Weg zu mehr Kontrolle und Vertrauen – ohne Verzicht auf Leistung oder globale Innovationskraft. Sie basiert vollständig auf der Microsoft EU Data Boundary, die garantiert, dass Kundendaten ausschließlich innerhalb der EU verarbeitet werden. Ergänzend sorgen External Key Management, Data Guardian und Regulated Environment Management für zusätzliche technische und operative Souveränität und schaffen eine belastbare Grundlage für sichere Cloud-Architekturen.

Transparenz: Unternehmen behalten die Hoheit über ihre Verschlüsselungsschlüssel, während Zugriffe durch Microsoft-Administratoren ausschließlich in Europa autorisiert, überwacht und in einem manipulationssicheren Ledger protokolliert werden. Diese Transparenz schafft klare Nachvollziehbarkeit aller administrativen Aktionen und stärkt die Nachweisfähigkeit gegenüber Auditoren, Aufsichtsbehörden und internen Compliance-Stellen.

Nahtlosigkeit: Die Sovereign Public Cloud erfordert keine Migration in separate Rechenzentren. Bestehende Azure-Regionen werden einfach um Souveränitätsfunktionen erweitert. Dadurch bleibt der gesamte Funktionsumfang von Microsoft 365, Azure und Dynamics 365 – inklusive modernster KI-Services – vollständig erhalten, während Datenschutz-, Sicherheits- und Governance-Anforderungen konsequent erfüllt werden. Der Übergang erfolgt schnell und ohne Technologiebruch.

Eignung: Damit ist die Sovereign Public Cloud ideal für Organisationen, die europäische Datenschutz- und Compliance-Vorgaben zuverlässig erfüllen möchten und gleichzeitig auf globale Innovationskraft, Skalierbarkeit und hohe Performance angewiesen sind. Sie verbindet regulatorische Klarheit mit modernster Technologie und wird so zum zukunftssicheren Sicherheitsfundament für Unternehmen jeder Größe.

Ihr Sicherheitsfundament

Stufe 1: Sovereign Public Cloud im Detail (Azure)

Herzstück der Sovereign Public Cloud sind drei technische Komponenten, die Datensouveränität und Kontrolle auf eine neue Stufe heben: External Key Management, Data Guardian und Regulated Environment Management. Gemeinsam bilden sie die Grundlage für ein Cloud-Modell, das Sicherheit, Compliance und Innovation vereint.

- **External Key Management (EKM)** ermöglicht es Unternehmen, ihre Verschlüsselungsschlüssel außerhalb der Microsoft-Cloud zu generieren, zu speichern und zu verwalten – beispielsweise in eigenen Rechenzentren oder bei zertifizierten Drittanbietern wie Futurex, Thales oder Utimaco. Die Schlüssel bleiben dabei vollständig im Besitz des Kunden, während sie dennoch mit Azure-Diensten genutzt werden können. Diese Trennung von Datenspeicherung und Schlüsselhoheit erfüllt zentrale regulatorische Vorgaben, etwa aus DSGVO, NIS2 und branchenspezifischen Compliance-Richtlinien. Unternehmen behalten so die volle Kontrolle über Zugriff und Entschlüsselung, während Microsoft technisch von der Vertrauenskette ausgeschlossen bleibt.
- **Data Guardian** sorgt für Transparenz und Aufsicht im Cloud-Betrieb. Zugriffe von Microsoft-Administratoren auf Systeme mit europäischen Kundendaten dürfen nur von Mitarbeitenden mit Wohnsitz in Europa autorisiert und in Echtzeit überwacht werden. Jeder Zugriff wird protokolliert und in einem manipulationssicheren Azure Confidential Ledger dokumentiert. So entsteht ein revisionssicherer Audit-Trail, der nicht nur regulatorische Anforderungen erfüllt, sondern auch das Vertrauen in den Cloud-Betrieb stärkt. Unternehmen wissen jederzeit, wer wann worauf zugegriffen hat – ein entscheidender Fortschritt gegenüber klassischen Public-Cloud-Modellen.
- **Regulated Environment Management (REM)** schließlich bietet eine zentrale Steuerungsschicht für alle Souveränitätsfunktionen. Über ein einheitliches Dashboard lassen sich Richtlinien für Data Guardian, Schlüsselmanagement, Confidential Computing und Compliance-Monitoring definieren und verwalten. REM visualisiert die Einhaltung von Standort- und Verschlüsselungsvorgaben, zeigt aktive Zugriffssitzungen und erstellt Nachweise für interne oder externe Audits. Damit wird Souveränität nicht nur technisch umgesetzt, sondern operativ steuerbar und prüfbar.

Gemeinsam ermöglichen diese Funktionen eine souveräne Cloud-Nutzung im europäischen Rechtsraum – mit maximaler Transparenz, nachweisbarer Kontrolle und ohne Einschränkung der Cloud-Funktionalität. Unternehmen behalten die Entscheidungshoheit über ihre Daten, Prozesse und Schlüssel – und gewinnen gleichzeitig die Agilität und Innovationskraft der Microsoft-Cloud.

Azure Local Systeme – „Made in Germany“

Stufe 2: Sovereign Private Cloud (Azure Local)

Die Sovereign Private Cloud richtet sich an Organisationen, die höchste Anforderungen an Betriebshoheit, Datensicherheit und Unabhängigkeit stellen. Sie basiert auf Azure Local – der Weiterentwicklung von Azure Stack HCI – und ermöglicht den Betrieb zentraler Microsoft-Cloud-Dienste im eigenen oder landeseigenen Rechenzentrum. Damit erhalten Unternehmen und Behörden dieselbe technologische Basis wie in der Public Cloud, jedoch mit vollständiger Kontrolle über Infrastruktur, Daten und Zugriffe.

Azure Local vereint Compute, Storage und Netzwerk in einer hyperkonvergenten Infrastruktur, die direkt mit der Microsoft-Cloud verbunden ist. Organisationen können zwischen hybriden und vollständig isolierten (air-gapped) Betriebsmodellen wählen. Im hybriden Modus profitieren sie von automatisierten Updates, zentralem Management und nahtloser Integration in Azure Services. Im isolierten Modus bleiben Systeme physisch und logisch getrennt – ein entscheidender Vorteil für KRITIS-Betreiber, öffentliche Einrichtungen oder den Finanzsektor, wo maximale Resilienz und Compliance Pflicht sind.

Die **Sovereign Private Cloud** ermöglicht die Nutzung vertrauter Dienste wie Azure Virtual Desktop, Azure Kubernetes Service oder Microsoft 365 Local, das Exchange Server und SharePoint Server in souveränen Umgebungen bereitstellt. So können auch sensible Daten und Fachanwendungen produktiv genutzt werden, ohne die eigene Sicherheits- oder Compliance-Architektur zu verlassen.

Technisch basiert Azure Local auf zertifizierter Hardware führender deutscher Partner wie TAROX, Thomas-Krenn oder Pyramid Computer. Jede Plattform durchläuft strenge Tests und erfüllt Microsoft-Standards für Performance, Redundanz und Verschlüsselung. Dadurch bleibt die Lösung kompatibel zur globalen Azure-Plattform, gleichzeitig aber vollständig unter lokaler Kontrolle.

Mit der Sovereign Private Cloud schaffen Organisationen ein souveränes Cloud-Ökosystem nach ihren eigenen Regeln – flexibel skalierbar, sicher nachweisbar und ohne Abhängigkeit von ausländischer Rechtsordnung. Sie verbindet die Vorteile der Cloud mit der Sicherheit eines national betriebenen Rechenzentrums – für souveräne IT-Infrastrukturen made in Germany.

Azure Local Systeme – „Made in Germany“

Stufe 2: Sovereign Private Cloud (Azure Local)

Die technologische Basis der Sovereign Private Cloud bilden in Deutschland gefertigte, von Microsoft zertifizierte Azure Local Systeme. Hersteller wie Pyramid Computer (Freiburg) liefern mit der AKHET-Serie hochverfügbare Serverplattformen, die exakt auf den Betrieb von Azure Local 24H2 und Windows Server 2025 abgestimmt sind.

- Die Systeme sind für den Rack-Betrieb in Rechenzentren konzipiert und verbinden industrielle Fertigungsqualität mit Cloud-Kompatibilität. Das kompakte 1U-Design (438 × 770 × 43 mm, ca. 20 kg) beherbergt Dual Intel Xeon Scalable Prozessoren (6. Gen), bis zu 2 TB DDR5 ECC-Speicher und bis zu zwölf Hot-Swap-Laufwerke für NVMe- oder SAS-SSDs. Damit lassen sich selbst rechenintensive Anwendungen und Virtualisierungsszenarien zuverlässig abbilden.
- Für Netzwerk-Performance sorgen Broadcom- oder Intel-Netzwerkkarten mit bis zu 200 GbE-Konnektivität; redundante 1600-W-Titanium-Netzteile sichern den Dauerbetrieb. Die Systeme unterstützen IPMI 2.0 Remote Management mit KVM-Funktion, wodurch Administration und Wartung vollständig remote erfolgen können – auch in abgeschotteten Umgebungen.
- Zertifizierungen nach CE und FCC sowie der Einsatz in DIN-Standard-19-Zoll-Racks machen die Hardware für den Einsatz in Behörden- und KRITIS-Infrastrukturen geeignet. Optional lassen sich die Systeme mit VMware ESXi 8.0 oder Proxmox VE betreiben, was hybride und isolierte Szenarien gleichermaßen unterstützt.

Damit verkörpern die Azure Local Systeme souveräne Cloud-Technologie „Made in Germany“: maximale Performance, geprüfte Sicherheit und eine nahtlose Einbindung in die Microsoft-Sovereign-Cloud-Architektur. Dank nationalem Betrieb und klarer Datenhoheit eignen sie sich ideal für sensible, regulierte Umgebungen und schaffen eine verlässliche Basis für moderne souveräne Cloud-Infrastrukturen.

Volle Kontrolle

Stufe 3: National Partner Cloud (Delos Cloud)

Die National Partner Cloud bildet die höchste Stufe des abtis Sovereignty Spectrum. Sie richtet sich an Organisationen, die maximale Kontrolle und vollständige Unabhängigkeit von ausländischer Einflussnahme benötigen – etwa öffentliche Verwaltungen, Körperschaften des öffentlichen Rechts und Betreiber kritischer Infrastrukturen.

Mit der Delos Cloud steht in **Deutschland erstmals eine nationale Cloud-Plattform** zur Verfügung, die auf Microsoft Azure-Technologie basiert, jedoch technisch, operativ und rechtlich souverän betrieben wird. Eigentümerin und Betreiberin ist die Delos Cloud GmbH, eine 100-prozentige Tochter der SAP SE. Microsoft fungiert ausschließlich als Technologielieferant; die operative Kontrolle liegt vollständig bei Delos.

Die Plattform ist darauf ausgelegt, die Cloud Platform Requirements (CPR) des Bundesamts für Sicherheit in der Informationstechnik (BSI) vollständig zu erfüllen. Alle Daten werden ausschließlich in Deutschland verarbeitet und nach nationalem Recht geschützt – ohne Zugriffsmöglichkeiten Dritter oder extraterritorialer Gesetze wie den US CLOUD Act. Damit ist Delos die erste Cloud-Lösung, die eine vollständige digitale Souveränität nach deutschem Standard gewährleistet.

Für die öffentliche Verwaltung bietet die Delos Cloud ein vertrautes Technologie-Ökosystem: Office 365 für Zusammenarbeit und Kommunikation, Azure-Dienste für Infrastruktur und Entwicklung, sowie SAP-Anwendungen für den Betrieb geschäftskritischer Systeme. Gleichzeitig unterstützt sie Fachanwendungen, Open-Source-Lösungen und hybride Szenarien im Rahmen der Deutschen Verwaltungscloud-Strategie (DVS).

Die Delos Cloud wird nach BSI C5, ISO 27001 und IT-Grundschutz zertifiziert und perspektivisch für den Geheimhaltungsgrad VS-NfD („Verschlusssache – Nur für den Dienstgebrauch“) qualifiziert. Damit ist sie die erste nationale Plattform, die Behörden, Kommunen und KRITIS-Betreibern einen rechts- und datensouveränen Cloud-Betrieb auf Enterprise-Niveau ermöglicht.

Mit abtis als Implementierungspartner profitieren Organisationen zusätzlich von praxisnaher Einführungserfahrung, bewährten Migrationskonzepten und umfassender Integration von Microsoft- und SAP-Diensten. So wird die National Partner Cloud zum sicheren Fundament einer souveränen digitalen Verwaltung – verankert in Deutschland, verbunden mit Europa, geschützt vor globalen Risiken.

Volle Kontrolle

Stufe 3: National Partner Cloud (Delos Cloud)

Die Delos Cloud unterscheidet sich von klassischen Public-Cloud-Angeboten vor allem durch ihr konsequent souveränes Betriebs- und Sicherheitsmodell.

Betrieb & Changes: Delos trennt Betrieb und Verantwortung strikt vom Public-Cloud-Modell: sicherheitsrelevante Änderungen laufen durch behördentaugliche Freigaben, mit Vorankündigung, definierten Release-Fenstern und Rollback-Pfad – ausgelegt für KRITIS und Verwaltung.

Identitäten & Zugriffe: Föderierte Entra-ID/AD-Modelle bleiben führend; privilegierte Zugriffe sind zeitlich befristet (PIM/JIT), begründet und vollständig protokolliert. Notfallzugriffe folgen einem Break-Glass-Prozess mit nachgelagerter Prüfung.

Netz & Jurisdiktion: Anbindungen erfolgen über dedizierte, verschlüsselte Verbindungen und getrennte Zonen. Telemetrie, Management und Datenverkehr bleiben national; Ausleitungen in Drittländer sind technisch und vertraglich ausgeschlossen.

Krypto & Nachvollziehbarkeit: Customer-Managed Keys in deutschen (Managed) HSMs sind Standard für sensible Daten. Alle Admin-Sitzungen werden manipulationsresistent geloggt; Retention und Integrität sind prüffähig geregelt.

Servicekatalog & Compliance: Office 365, Azure- und SAP-Dienste werden souverän vorkonfiguriert (Region-Bindung, Verschlüsselung, Hardening). Kunden erhalten prüffähige Artefakte (Policies, Baselines, Change-Protokolle) für IT-Grundschutz/BSI-C5/VS-NfD-Vorbereitung.

Migration mit abtis: Standardisierte Pfade nutzen Sovereign Landing Zones, Policy-as-Code und automatisierte Evidenzen für sichere Freigaben. Souveränität geht vor Funktionsbreite, einige Public-Cloud-Features folgen zeitversetzt – zugunsten maximaler Rechts- und Betriebshoheit und einer klar planbaren Roadmap.

Öffnungsklausel: Delos Cloud und Microsoft haben vereinbart, dass Kunden bei einem EU-weiten Bereitstellungsverbot für Microsoft-Cloud-Dienste sicher auf die nationalen Delos-Cloud-Dienste migrieren können. Ein spezieller Zugriff auf Microsoft-Code gewährleistet zusätzlich die operative Handlungsfähigkeit von Delos Cloud.

Die Delos Cloud bietet eine souveräne, national kontrollierte Cloud-Plattform mit strikt getrenntem Betrieb, hoher Sicherheit und vollständiger Compliance. Sie liefert maximalen Schutz und Nachvollziehbarkeit für Behörden und KRITIS, während abtis klare, standardisierte Migrationspfade für eine sichere und effiziente Einführung bereitstellt.

Sichere Alternative aus der EU

Europäische Cloud-Landschaft: Anspruch und Realität

Der Ruf nach digitaler Souveränität führt viele Unternehmen dazu, europäische Cloud-Alternativen zu prüfen. Doch der Blick auf den Markt zeigt schnell: Während europäische Anbieter wichtige Impulse setzen, sind sie funktional und wirtschaftlich noch weit von der Leistungsfähigkeit moderner Hyperscaler entfernt.

Starke Infrastruktur, schwache Plattform: Die meisten europäischen Clouds liefern solide Infrastruktur – virtuelle Maschinen, Storage, Netzwerke. Was jedoch fehlt, sind die Plattformdienste, die moderne Cloud-Betriebsmodelle prägen: Serverless, KI-Services, integrierte Sicherheit, Observability oder Identity-Lösungen. Unternehmen müssen vieles wieder selbst betreiben – mit höherem Aufwand, mehr Komplexität und geringerer Automatisierung.

Mehr Verantwortung, höhere Kosten: Ohne echte Pay-per-Use-Modelle oder skalierende Plattformdienste basieren viele EU-Angebote weiterhin auf festen Ressourcenpaketen. Das macht den Betrieb nicht nur schwerfälliger, sondern oft auch deutlich teurer. Wo Hyperscaler flexibel und verbrauchsabhängig abrechnen, verlangen europäische Anbieter häufig klassische Sizing-Modelle – inklusive permanenter Kosten selbst für wenig genutzte Anwendungen.

Souveränität ist kein Entweder-oder: Europäische Clouds leisten einen wichtigen Beitrag zur Unabhängigkeit – aber sie ersetzen die Innovationsgeschwindigkeit, Effizienz und Tiefe globaler Cloud-Ökosysteme nicht. Wer echte digitale Souveränität erreichen will, braucht deshalb keine Schwarz-Weiß-Entscheidung, sondern einen Ansatz, der Stärken kombiniert: nationale Hoheit dort, wo sie zwingend ist, und globale Leistungsfähigkeit dort, wo sie wirtschaftlich und technologisch notwendig bleibt.

Digitale Souveränität entsteht nicht durch den Verzicht auf moderne Cloud-Technologie, sondern durch ihre bewusste Kombination. Europäische Anbieter schaffen wichtige Grundlagen für Kontrolle und Hoheit – doch echte Resilienz entsteht erst, wenn nationale Souveränität und globale Innovationskraft zusammenwirken. Der Schlüssel liegt in einem klugen Mix, der Sicherheit, Effizienz und Zukunftsfähigkeit gleichermaßen ermöglicht.

Zukunftssicher: Für Ihre Cloud-Strategie

abtis Workshop: Souveränität & Resilienz

Der abtis Workshop „**Souveränität & Resilienz**“ bietet Entscheidungsträgern eine kompakte und praxisorientierte Orientierungshilfe, um die eigene Cloud-Strategie auf Zukunftssicherheit und regulatorische Anforderungen auszurichten. In nur einem Tag erhalten Teilnehmende einen klaren, umsetzbaren Fahrplan zur Balance zwischen Cloud-Vorteilen, Compliance und digitaler Souveränität.

Im Mittelpunkt steht die **Analyse der aktuellen Cloud-Landschaft** anhand des Microsoft Cloud Adoption Frameworks. Dabei werden individuelle Anforderungen, Compliance-Vorgaben und Sicherheitsbedarfe systematisch bewertet. Auf dieser Basis erarbeitet abtis gemeinsam mit dem Kunden ein maßgeschneidertes Zielbild – inklusive Governance-Ansatz und Business-Continuity-Konzept.

Der Workshop vermittelt ein fundiertes **Verständnis der drei Souveränitätsdimensionen** nach Gartner – Daten-, operative und technologische Souveränität – und zeigt konkrete Lösungsoptionen im Microsoft-Ökosystem: von der Public Cloud über Azure Local bis hin zur Delos Cloud. Teilnehmende erhalten zudem eine Einschätzung, wie Microsofts European Digital Commitments und das abtis Sovereignty Spectrum für ihr Unternehmen relevant sind.

Am Ende steht ein klares Ergebnis: ein High-Level-Konzept mit konkreten Handlungsempfehlungen, einer Preisindikation für die Umsetzung und klar definierten nächsten Schritten. Der Workshop richtet sich an IT-Entscheider, Datenschutzverantwortliche und Sicherheitsbeauftragte, die Cloud-Innovationen souverän gestalten möchten – sicher, compliant und skalierbar.

Zum Workshop

Souveränität als Kern moderner Unternehmensstrategie

Strategischer Nutzen – Souverän. Sicher. Zukunftsfähig.

Die souveräne Cloud stärkt die digitale Handlungsfähigkeit von Unternehmen und öffentlichen Organisationen. Sie schafft die Grundlage, um Innovation mit Sicherheit zu verbinden – und das auf europäischer Rechts- und Wertebasis. Durch **klare Kontrolle über Daten, Zugriffe und Schlüssel** behalten Organisationen jederzeit die Hoheit über ihre Informationen und Systeme.

Souveränität bedeutet in diesem Kontext mehr als Datenschutz: Sie ist ein strategisches Instrument zur Risikominimierung. Durch den Betrieb innerhalb der EU Data Boundary und die Möglichkeit, Verschlüsselungsschlüssel außerhalb der Cloud zu verwalten, entfallen rechtliche Unsicherheiten und Abhängigkeiten von Drittländern. Unternehmen gewinnen damit volle Transparenz und Kontrolle – technisch, organisatorisch und rechtlich.

Sicherheit ist dabei integraler Bestandteil. Die abtis Gruppe stellt mit ihrem **24/7 Managed Security Operations Center (MXDR)** und der Zero-Trust-Architektur einen durchgängigen Schutz der Cloud-Umgebungen sicher. Als Mitglied der Microsoft Intelligent Security Association (MISA) verfügt abtis über direkten Zugriff auf aktuelle Bedrohungsinformationen und Sicherheitsinnovationen – für proaktive Abwehr und kontinuierliche Überwachung.

Gleichzeitig sorgt die souveräne Cloud für Resilienz in einer zunehmend unsicheren Welt. Sie schützt vor geopolitischen Risiken, erfüllt europäische Regularien wie DORA, NIS2 und AI Act und stellt sicher, dass kritische Daten und Prozesse auch im Krisenfall handlungsfähig bleiben. Damit wird Souveränität zum zentralen Baustein digitaler Zukunftsfähigkeit – eine strategische Entscheidung für Sicherheit, Stabilität und Vertrauen.

Die souveräne Cloud verbindet Innovation mit europäischer Sicherheit und gibt Organisationen volle Kontrolle über ihre Daten. Sie reduziert rechtliche und geopolitische Risiken, erhöht die Resilienz und erfüllt zentrale EU-Regularien. Mit ganzheitlichen Sicherheitsdiensten wie dem 24/7 MXDR-SOC der abtis Gruppe wird sie zum strategischen Fundament für eine vertrauenswürdige und zukunftsfähige digitale Transformation.

Operative Exzellenz durch Souveränität

Operativer Nutzen – Messbar. Skalierbar. Praxisbewährt

Die souveräne Cloud entfaltet ihren Mehrwert nicht nur auf strategischer, sondern auch auf operativer Ebene – durch höhere Effizienz, Flexibilität und messbare Resultate im Tagesgeschäft. Unternehmen profitieren von einer Infrastruktur, die sich dynamisch an ihre Anforderungen anpasst: vom souveränen Public-Cloud-Modell bis hin zur vollständig nationalen Cloud-Instanz – ohne Technologiebruch, Funktionsverlust oder organisatorische Reibung.

Compliance by Design stellt sicher, dass Datenschutz, Sicherheit und Nachweisführung nicht nachträglich implementiert werden müssen, sondern von Beginn an integraler Bestandteil des Betriebs sind. Automatisierte Richtlinien, Policy-as-Code, souveräne Identitätsmodelle und vertrauliche Datenverarbeitung mit Confidential Computing garantieren, dass regulatorische Vorgaben jederzeit eingehalten und revisionsfest dokumentiert werden – ohne zusätzlichen Aufwand für IT, Datenschutz oder Revision.

Gleichzeitig steigert die souveräne Cloud Produktivität und Innovationsgeschwindigkeit. Lösungen wie Microsoft 365 Local, Azure AI und Copilot können souverän, datenschutzkonform und sicher betrieben werden – sodass Teams ortsunabhängig, effizient und kollaborativ arbeiten können. Durch standardisierte Landing Zones, automatisierte Governance und erprobte Migrationspfade verkürzt sich die Einführung neuer Cloud-Services um bis zu 30 Prozent, bei konstant hohem Sicherheits- und Compliance-Niveau.

Mit ihrer **modularen Architektur** bietet die souveräne Cloud eine belastbare Grundlage für skalierbares Wachstum und nachhaltige Digitalisierung. Unternehmen können Innovationen schnell ausrollen, neue Dienste sicher integrieren und ihre Infrastruktur flexibel erweitern – ohne Kompromisse bei Datenschutz, Governance oder Leistung einzugehen. So verbindet sie die Agilität moderner Cloud-Technologien mit der Stabilität klassischer IT und wird zum Motor einer resilienten, zukunftsfähigen digitalen Infrastruktur.

Der Einstieg gelingt praxisnah über den Workshop „**Souveränität & Resilienz**“, der in wenigen Tagen einen klaren Fahrplan zur sicheren und skalierbaren Cloud-Nutzung liefert. So wird Souveränität messbar – in Effizienz, Sicherheit und Innovationskraft.

Die souveräne Cloud steigert Effizienz, Produktivität und Compliance zugleich. Sie ermöglicht schnelle, sichere Innovationen, automatisierte Governance und flexible Skalierbarkeit – ohne Kompromisse bei Datenschutz oder Leistung. So wird sie zur stabilen und zugleich agilen Basis für eine zukunftsfähige digitale Infrastruktur.

Auszeichnung für Digitale Resilienz

Microsoft Partner of the Year Award 2025

Mit der Auszeichnung als Microsoft Partner of the Year 2025 in der Kategorie Act to Accelerate Digital Resilience gehört abtis zu den europaweit führenden Experten für souveräne Cloud-Architekturen. Der Award würdigt unseren Beitrag, Organisationen in Deutschland und Europa zu mehr digitaler Souveränität, Sicherheit und Resilienz zu führen – und zeigt, wie relevant der souveräne Weg in die Cloud geworden ist.

Anerkennung für souveräne Cloud-Strategien – made in Germany. Die Auszeichnung bestätigt die besondere Stärke von abtis: technische Exzellenz, tiefes Verständnis regulatorischer Anforderungen und ein souveränes Cloud-Portfolio, das sich konsequent an europäischen Werten orientiert. Mit dem Sovereignty Spectrum bietet abtis ein klar strukturiertes Modell, das Unternehmen Schritt für Schritt zu ihrer optimalen Form digitaler Souveränität führt – von der Sovereign Public Cloud über Azure Local bis hin zur Delos Cloud.

Souveränität als Treiber digitaler Resilienz. Ob Mittelstand, KRITIS oder öffentlicher Sektor – abtis hilft Organisationen, Cloud-Innovation mit Sicherheit, Compliance und Transparenz zu verbinden. Durch Technologien wie External Key Management, Data Guardian, Confidential Computing und Microsoft 365 Local unterstützen wir Unternehmen dabei, Datenhoheit, Betriebssicherheit und regulatorische Anforderungen souverän umzusetzen. Der Award unterstreicht, wie konsequent abtis diese Themen verbinden und damit einen spürbaren Mehrwert schafft.

Signalwirkung für Europas digitale Zukunft. Der Award ist ein Zeichen dafür, dass digitale Resilienz und souveräne Cloud-Modelle zu entscheidenden Erfolgsfaktoren Europas werden. Im Umfeld der neuen European Digital Commitments und der Microsoft Sovereign Cloud trägt abtis maßgeblich dazu bei, europäische Stabilität, Datenschutz und technologische Unabhängigkeit zu stärken. Damit entwickelt sich abtis zu einem der wichtigsten Wegbereiter für souveräne, sichere und skalierbare Cloud-Infrastrukturen in Deutschland und Europa.

Security Expertise der Spitzenklasse

Schutz, der souveräne Cloud möglich macht

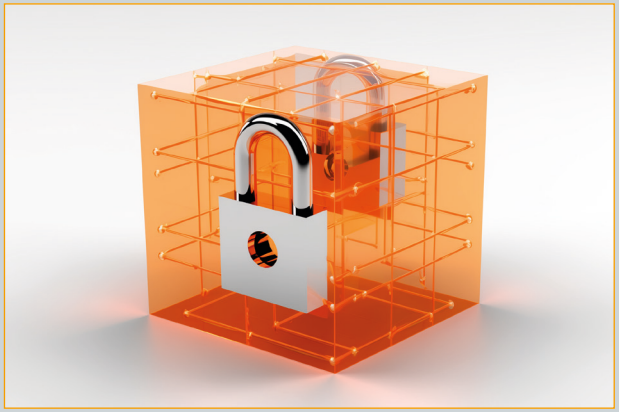
Sicherheitsfundament: Souveräne Cloud benötigt Sicherheit als Grundprinzip, nicht als Zusatz. Genau hier setzt abtis an: mit tiefem Microsoft-Know-how, einem konsequenten Zero-Trust-Ansatz und einem vollständig in Deutschland betriebenen Security Operations Center. Unsere Mitgliedschaft in der Microsoft Intelligent Security Association und verifizierte MXDR-Dienste positionieren abtis als einen der führenden Security-Partner für resiliente Cloud-Umgebungen in Europa.

Erkennen & Reagieren: Unser MXDR-Service überwacht Identitäten, Endpoints, Infrastruktur und Cloud-Workloads rund um die Uhr. KI-gestützte Analysen in Microsoft Sentinel identifizieren Angriffe frühzeitig, während automatisierte Response-Prozesse die Eindämmung erheblich beschleunigen. So entsteht die Transparenz und Handlungssicherheit, die souveräne Architekturen erfordern.

Zero Trust als Prinzip: Wir stärken Identitäten, reduzieren Berechtigungen auf das Minimum und sichern kritische Prozesse durchgehender. Segmentierung, starke Authentifizierung und moderne Microsoft-Security-Plattformen sorgen dafür, dass sich souveräne Public-, Private- und National-Cloud-Modelle kontrolliert und sicher betreiben lassen.

Incident Response & Härtung: Kommt es zu einem Sicherheitsvorfall, übernimmt unser deutsches SOC mit klar definierten Incident-Response- und Forensik-Prozessen. Analyse, Ursachenbehebung und nachhaltige Härtung greifen nahtlos ineinander – für schnelle Wiederherstellung und langfristige Resilienz.

Ganzheitliche Resilienz: Penetrationstests, Security-Awareness-Programme und Governance-Frameworks für NIS2, DORA, KRITIS oder ISO-Standards runden unseren Ansatz ab. So entsteht ein Sicherheitsrahmen, der Compliance, Kontrolle und Geschwindigkeit verbindet – und souveräne Cloud-Transformation wirklich möglich macht.



Microsoft Azure Specialist for ISV

Microsoft Fast Track Partner

Microsoft Partner

Infra and Database Migration
Hybrid Cloud Infrastructure
Kubernetes on Microsoft Azure
Azure Virtual Desktop
Analytics
Modernize Endpoints
Small and Midsize Business Management

Meetings and Meeting Rooms for Microsoft Teams
Teamwork Deployment
Calling for Microsoft Teams
Indentity and Access Management
Cloud Security
Threat Protection
Information Protection and Governance
Adoption and Change Management

DELOS CLOUD DELL Technologies PYRAMID utimaco®

[abtis]
DIGITALE ZUKUNFT

Lassen Sie uns gemeinsam Ihre Digitale Zukunft gestalten

Die abtis Gruppe führt als IT-Dienstleister den Mittelstand mit strategischer Beratung, effizienten Projekten und maßgeschneiderten Managed Services sicher in die digitale Zukunft. Die Gruppe verfügt über mehr als 20 Jahre Erfahrung in der Planung, der Umsetzung und dem Betrieb von Microsoft-Plattformen. Sie betreut bereits mehr als 250.000 Anwender der Cloud-Plattformen Microsoft 365 und Azure. Die abtis Gruppe ist Mitglied der Microsoft Intelligent Security Association (MISA), Fokuspartner von Microsoft für den Mittelstand sowie Gewinner des Microsoft Accelerate Innovation Awards 2023 und des Microsoft Act to Accelerate Digital Resilience Awards 2025. Dabei deckt abtis alle Lösungsbereiche von Microsoft ab: von Modern Work über Security, Business Applications, Infrastructure (Azure), Digital & App Innovation (Azure) bis hin zu Data & AI (Azure).

[abtis] CETERIS AG changeable

Nehmen Sie Kontakt mit uns auf.

www.abtis.de +49 7231 4431 - 100 vertrieb@abtis.de

abtis Holding AG • Wilhelm-Becker-Straße 11b • 75179 Pforzheim

Genderhinweis: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

© 2026 Alle Rechte vorbehalten. Dieses Dokument ist urheberrechtlich geschützt. Sämtliche Inhalte dienen der Dokumentation. Jede andere Nutzung, insbesondere die Weitergabe an Dritte, die Verbreitung oder die Bearbeitung, auch in Teilen, ist ohne schriftliche Einwilligung der abtis Holding AG untersagt. Die verwendeten Firmen-, Marken- und Produktnamen und Warenzeichen sind eingetragene Markenzeichen oder Warenzeichen der jeweiligen Inhaber und werden hiermit anerkannt.