novaCapta

eBook

German Angst & Cloud: Sicherheit neu gedacht

Was hinter der deutschen Skepsis steckt – und wie Unternehmen dennoch souverän die Cloud nutzen können

DE

novaCapta GmbH
Im Mediapark 5c
50670 Köln

T +49 (0)221 58919 343
M info@novacapta.com
W www.novacapta.de

CH

novaCapta Schweiz AG
Theaterstrasse 17
8400 Winterthur

T +41 (0)41 392 20 00
M info.schweiz@novacapta.com
W www.novacapta.ch

Die Angst vor Kontrollverlust, Spionage oder unvorhersehbaren Kosten macht vielen deutschen Entscheidern den Umstieg in die Cloud schwer.

Doch moderne Technologien, europäische Regularien und globale Marktmechanismen sorgen längst für mehr Sicherheit, als oft angenommen.

Dieses eBook räumt mit Vorurteilen auf und gibt klare Orientierung für eine fundierte souveräne Cloud-Strategie – jenseits der (German) Angst.

Autor: Jürgen Dick

Jürgen Dick ist ein erfahrener Cloud-Architekt & IT-Stratege mit tiefgreifendem Know-how in der Entwicklung und Umsetzung von Cloud- und Infrastrukturprojekten im Microsoft-Umfeld.

Seit rund 25 Jahren begleitet er Unternehmen dabei ihre IT-Landschaften zukunftssicher und compliance-konform in die Cloud zu überführen. Seine beruflichen Stationen, u.a. bei Microsoft, haben ihn zu einem anerkannten Experten im Bereich Microsoft Azure, Hybrid-Cloud-Szenarien und Governance-Frameworks gemacht. Dabei versteht er es, komplexe regulatorische Anforderungen mit den technologischen Möglichkeiten von Microsoft 365, Azure und der Sovereign Cloud Strategie in Einklang zu bringen.

Bei der novaCapta setzt Jürgen Dick als Leiter der Unit Cloud Security und Infrastructure seine Expertise im Aufbau souveräner Cloud-Infrastrukturen gezielt in Kundenprojekten ein und zeigt Unternehmen, wie sich die Vorteile der Cloud-Technologie nutzen lassen, ohne die Hoheit über eigene Daten aus der Hand zu geben.

novaCapta

novaCapta ist Ihr Partner für die digitale Transformation mit Microsoft Technologien. Wir sind Treiber der digitalen Transformation und Zukunftsfähigkeit unserer Kunden.

Auf Basis von Microsoft Technologien entwickeln wir Lösungen, die Prozesse optimieren, Kosten senken, Produktivität stärken und damit den Erfolg unserer Kunden sichern.

Microsoft zeichnete uns dafür als Microsoft Solutions Partner „Microsoft Cloud" aus.

Wir bieten Ihnen eine ganzheitliche Technologieberatung und Lösungen für den Digital Workplace, die genau auf Ihre Anforderungen, Ziele und Herausforderungen zugeschnitten sind: Von der strategischen IT-Beratung, über Infrastruktur, Security, Kollaboration, Anwendungsentwicklung, Business Applications und KI-Lösungen bis hin zu Managed Services sowie Change & Adoption.

Einleitung

In einer Zeit, in der die Welt von Unsicherheit und Unruhe geprägt ist, scheint die deutsche Gesellschaft besonders anfällig für Ängste und Sorgen zu sein. Dieses Phänomen, als „German Angst" bezeichnet, hat laut Wissenschaftler:innen tiefe historische Wurzeln und spiegelt eine kollektive Sorge und Sensibilität gegenüber Bedrohungen und Risiken sowie eine Zögerlichkeit im Angesicht von Veränderungen wider[1].

Die jüngsten geopolitischen Entwicklungen haben diese Ängste weiter angeheizt. Konflikte an den Grenzen Europas, wirtschaftliche Turbulenzen und die wachsende Bedrohung durch globale Krisen haben die deutsche Bevölkerung und Wirtschaft in einen Zustand erhöhter Wachsamkeit und Besorgnis versetzt. Die German Angst zeigt sich auch stets gegenüber dem Aufkommen neuer und revolutionärer Technologien (man denke zum Beispiel an die enorme Skepsis gegenüber Social Media Ende der 2000er und Anfang der 2010er Jahre). Den Deutschen wird attestiert, dass sie zuerst nach den möglichen Risiken fragen, statt die Vorteile zu sehen.

Aktuell lässt sie sich dies auch bei der Nutzung von Cloud-Technologien durch Unternehmen und öffentliche Einrichtungen beobachten – vor allem, wenn die Cloud-Anbieter nicht EU-Unternehmen sind.

Einige Entscheider:innen in Unternehmen und Organisationen haben ein ungutes Bauchgefühl und fürchten sich vor Sicherheitsrisiken und/oder Datenverlust, die mit der Cloud-Nutzung verbunden sein könnten. Dazu kommt die Angst, durch einfache „Dekrete" von Regierungen anderer Länder könnte der Zugriff auf die eigenen Daten verloren gehen oder durch neue Zölle in den gegenseitigen Handelsbeziehungen könnten die Kosten ins unermessliche steigen. Viele dieser Ängste sind jedoch unbegründet, da moderne technische Lösungen und Sicherheitsvorkehrungen diese Risiken effektiv minimieren können.

Ebenso habe ich hohes Vertrauen in die Durchsetzungskraft der Europäischen Union und der Zusammenarbeit mit weltweit agierenden „Hyperscalern". Wirtschaftlich betrachtet steuert Europa bei den meisten dieser Unternehmen, laut eigener Quartalsgeschäftsberichte, im Schnitt über 40% des Umsatzes bei. Basierend auf meiner 30-jährigen Erfahrung in der IT-Branche, bin ich mir sicher, dass kein amerikanisches Unternehmen auf diesen Umsatz so „mir-nichtsdirnichts" verzichten will.

Aber zurück zur technischen Sichtweise: Durch die richtige Implementierung und Verwaltung von Cloud-Technologien können Unternehmen nicht nur ihre Effizienz steigern, sondern auch ihre Daten sicher und geschützt halten (auf Wunsch sogar mit „Deutscher Sicherheitstechnologie" inklusive Freigabe durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) – sprich VS-NfD konform.

Ein weiteres Thema, was diesbezüglich deutsche Unternehmen beschäftigt, ist die Frage, ob sie lieber lokale Cloud-Anbieter (z. B.StackIT, OTC, IONOS) statt amerikanischer nutzen sollten.

[1]**Mehr dazu:** Historiker Frank Biess forscht an der University of San Diego zur Entwicklung der kollektiven deutschen Angst ab 1945. In seinem Buch „Republik der Angst. Eine andere Geschichte der Bundesrepublik" sowie in einem gleichnamigen Vortrag an der Universität Tübingen am 22. Juli 2021 (Mitschnitt bei Deutschlandfunk) , hat er seine Erkenntnisse geteilt.

Eine Entscheidung für einen dieser Anbieter ist aber oft mit sehr hohen Kompromissen verbunden, da lokale Anbieter bei weitem nicht die gleiche Funktionalität und Sicherheit bieten können wie die etablierten Hyperscaler, wie z. B. Microsoft, Amazon oder Google.

Unternehmen müssen daher sorgfältig abwägen, ob sie diese Einbußen in Kauf nehmen oder sich für bewährte Lösungen der größeren, internationalen Anbieter entscheiden.

Bemerkung:

Einmal abgesehen von dem hohen Unterschied des bestehenden Angebotes an Services zwischen Hyperscalern und lokalen Anbietern, sollte man etwas genauer hinsehe,n auf welcher Basis „lokale souveräne" Clouds entwickelt wurden. In fast allen Fällen werden Produkte von amerikanischen bzw. weiterer internationaler Firmen im eigenen Cloud-Basisangebot implementiert bzw. stehen als Add-On Technologie-Partnerlösung zur Verfügung (bspw. Hardware der Server, Virtualisierungslayer, Automatisierung, Data- und -Analyticslayer u.v.m). Somit gerät das Marketing-Boot dieser vermeintlich rein lokalen Cloud Provider doch etwas ins Wanken.

In einer zunehmend digitalisierten Welt stehen Regierungen und öffentliche Institutionen vor der Herausforderung, innovative Technologien (allen vorweg gerade Künstliche Intelligenz) zu nutzen, während sie gleichzeitig die Kontrolle über ihre sensiblen Daten behalten müssen. Seit vielen Jahren beschäftige ich mich mit den Möglichkeiten der Vor- bzw. Nachteile von Hyperscalern.

Mein Fazit ist allerdings, dass nur einer dieser das deutsche Enterprise Business, den Mittelstand und die öffentliche Hand wirklich verstanden und in diesem Zuge Möglichkeiten geschaffen hat, die Potenziale der Cloud effektiv und sicher zu nutzen.

Dieser Hyperscaler ist Microsoft mit seinen Onlinediensten Microsoft 365, Business Applications und Microsoft Azure. Deutlich wird dies seit längerem vor allem anhand der Anzahl der verfügbaren lokalen Rechenzentren, und noch mehr durch den klaren Fokus auf Sicherheit und Compliance. 2025 tritt Microsoft der Skepsis am europäischen Markt selbstbewusst entgegen und betont das Engagement, europäisches Recht zu vertreten und mit seinen Technologien zu schützen.

Die „Microsoft Sovereign Cloud“, die „EU Data Boundary“ und „Microsoft’s 5 Digital European Commitments“ sind drei herausstechende Beispiele für Microsofts Streben für die sichere Cloud in Europa und die Cloud nach europäischen Vorstellungen.

Der CLOUD Act: Treiber der „German Angst“

Der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) ist ein US-amerikanisches Gesetz, das im März 2018 verabschiedet wurde. Es verpflichtet US-basierte Cloud-Anbieter wie z. B. Microsoft, Amazon oder Google, auf **rechtmäßige Anfragen** von US-Strafverfolgungsbehörden zu reagieren und zwar unabhängig davon, wo sich diese Daten physisch befinden. Das bedeutet: Auch wenn Daten auf Servern außerhalb der USA gespeichert sind – etwa in Europa und in Deutschland können US-Behörden deren Herausgabe verlangen, sofern die Daten sich im „Besitz, Gewahrsam oder unter Kontrolle“ des US-Anbieters befinden.

Folgende Punkte sind wichtig zu wissen:

- Dieses Gesetz bezieht sich nur auf Strafrecht und nicht auf Zivilrecht
- Es muss sich um eine Straftat handeln, um einen nachvollziehbaren Durchsuchungsbefehl (durch einen unabhängigen Richter validiert) zu bekommen und die Daten müssen genau spezifiziert sein (Datentyp und Quelle)
- Eine solche richterlich beschlossene Herausgabe von Daten ist nichts Neues
- Es schließt explizit eine Verpflichtung des Providers zur Entschlüsselung der Daten aus

Beachtet werden in diesem Zusammenhang, die Richtlinien des Department of Justice (Leitfaden des DOJ: „Evaluation of Corporate Compliance Programs“). Diese helfen Strafverfolgungsbehörden bei der strafrechtlichen Verfolgung von Unternehmen, die gegen Gesetzte verstoßen (Schwerpunkte sind Bekämpfung von Kartellen, transnationaler krimineller Organisationen und Wirtschaftskriminalität), die die US-Interessen gefährden können.

Somit betrifft dieses Vorgehen ohnehin nicht die Unternehmen, die europäische sowie länderspezifische Gesetze befolgen. Microsoft agiert hier zudem sehr transparent und informiert detailliert über alle Richtlinien bezüglich Regierungsanfragen im Microsoft Data Law Blog.

Bemerkung:

Da ich nur Interessierter an diesem Thema bin aber kein Anwalt, empfehle ich Ihnen bei mehr Wissensbedarf, eine rechtliche Absicherung hinzuzuziehen. Fachanwälte können Ihnen zudem tiefgehende Einblicke geben in das Prinzip der Comitas Gentium (Principle of Comity), das bedeutet, dass Gerichte eines Staates die Gesetze und Urteile eines anderen Staates aus Respekt (nicht wegen rechtlicher Pflicht) anerkennen oder anwenden können. Diese spielen bei einer solchen Anfrage ebenso eine erhebliche Rolle.

Schlüsselfragen für eine sichere Cloudnutzung und Anbieterwahl

Zentrale Fragen, die Sie für sich beantworten sollten, um sicherzustellen, dass Sie Ihre Daten optimal schützen, regulatorische Anforderungen erfüllen und Ihre digitale Strategie effizient umsetzen können.

Vertrags- und Wartungsmodelle

- Wo ist der Gerichtsstand meines Vertragspartners? Es sollte unbedingt darauf geachtet werden, dass dieser innerhalb der EU liegt
- Stellt der ausgewählte Cloud-Anbieter erweiterte Verträge bereit, die das eigene Business und dessen spezifische Anforderungen absichern (z. B. für Banken, Versicherungen, Healthcare)?
- Gibt es genügend Auswahl an lokalen Beratungshäusern, die nicht nur technisch, sondern auch in Bezug auf Kosten und Verträge seriös beraten können?

Datenschutz & Sicherheit

- Welche Datenschutzbestimmungen gelten für meine Branche und Region und wie erfüllt meine Cloud diese Anforderungen (Integrität und Compliance von Clouddaten | Microsoft Trust Center)?
- Wo werden meine Daten gespeichert und verarbeitet? Bleiben sie innerhalb der EU, um DSGVO-Konformität zu gewährleisten (Analyse und Telemetriedaten eingeschlossen)?
- Welche Sicherheitsmechanismen bietet die Cloud, um meine Daten vor Cyberangriffen bzw. vor „ungewollten Mitlesenden“ zu schützen?

Kontrolle & Transparenz

- Habe ich die volle Kontrolle über meine Daten oder bin ich abhängig von bestimmten Cloud-Anbietern? Sofern ich abhängig bin, ist dieser Zustand in Ordnung für mich oder möchte ich mich noch unabhängiger machen?
- Kann ich nachvollziehen, wie meine Daten genutzt werden und wer Zugriff darauf hat?
- Welche Maßnahmen gibt es zur Verschlüsselung und Zugriffskontrolle?

Compliance & Rechtliche Aspekte

- Erfüllt die Cloud die gesetzlichen Vorgaben und Compliance-Anforderungen meines Unternehmens (z B. NIS2, ISO27001x, TISAX, C5 oder auch DORA für Banken und Versicherungen)?
- Gibt es spezielle Zertifizierungen und Audits, die die Souveränität der Cloud bestätigen? Es empfiehlt sich bei vertrauten Unternehmen im eigenen Industriezweig zu erkundigen. (Bitte keine falsche Scham an den Tag legen! Jede:r fängt mal an!)
- Wie wird der Zugriff von Aufsichtsbehörden oder Dritten geregelt?

Technische Infrastruktur & Integration

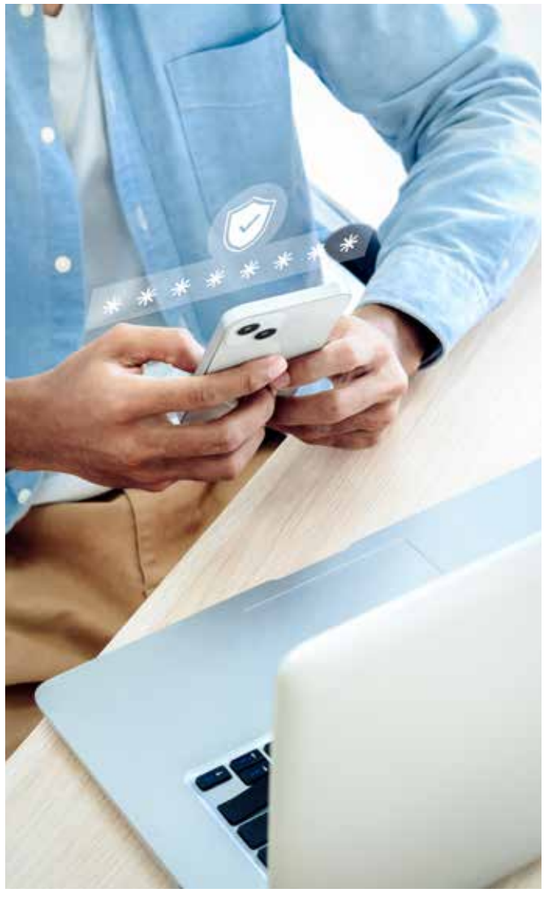
- Ist die Cloud mit meinen bestehenden IT-Systemen und Anwendungen kompatibel? In über 90% aller Projekte läuft es auf eine Hybride Cloudnutzung hinaus.
- Welche Flexibilität bietet die Cloud bei Skalierung und Anpassung an zukünftige Geschäftsanforderungen?
- Wie einfach ist die Migration von bestehenden Daten und Prozessen in eine neue Aufbau- und Ablauforganisation?

Kosten & Wirtschaftlichkeit

- Welche langfristigen Kosten und Einsparpotenziale für mein Business ergeben sich durch die Nutzung der Cloud und auch Künstlicher Intelligenz (z. B. Zeitaufwand bei Forschung und Entwicklung, Kundenzufriedenheit)?
  - Fragen wie “Ist mein Server mit 2 CPUs in der Cloud günstiger als im eigenen Rechenzentrum?“ sind dabei zu kurz gedacht und mit Blick auf das große Ganze nicht zielführend.
- Gibt es versteckte Kosten für zusätzliche Sicherheitsmaßnahmen oder Compliance-Anforderungen?
- Wie sehen der Support und die Wartung aus? Gibt es langfristige Verfügbarkeitsgarantien? Wie ist der Abkündigungszeitraum von Services geregelt?

Strategische Überlegungen

- Unterstützt die Cloud meine langfristige Unternehmensstrategie und digitale Transformation? Nutzen Sie Beratungshäuser, die amerikanische Marketingfolien von der Realität unterscheiden!
- Wie wirkt sich die Nutzung der Cloud auf meine Wettbewerbsfähigkeit aus?
- Bietet der Cloud-Anbieter regelmäßige Innovationen und Weiterentwicklungen für meine Branche? Hier sollte die gesamte Cloud Stack Themenpalette – vom Arbeitsplatz über Anwendungen/AI, Codeentwicklung, Datenanalysen hin zu Rechenzentren – beleuchtet werden!



Microsofts Data Boundary: Commitment gegenüber allen Kunden in der Europäischen Union

Mit der zunehmenden digitalen Vernetzung und den wachsenden Anforderungen an Datenschutz und Datenkontrolle spielt die EU Data Boundary von Microsoft eine entscheidende Rolle für europäische Unternehmen und öffentliche Institutionen.

Microsoft hat mit der EU Data Boundary eine branchenführende Lösung geschaffen, die sicherstellt, dass Kundendaten jeglicher Industriezweige, aber auch aus der öffentlichen Hand ausschließlich innerhalb der Europäischen Union (EU) und der Europäischen Freihandelsassoziation (EFTA) gespeichert und verarbeitet werden.

Diese Initiative ist ein bedeutender Meilenstein für den Schutz von Daten und die Einhaltung strenger europäischer Datenschutzvorgaben, insbesondere der Datenschutz-Grundverordnung (DSGVO).

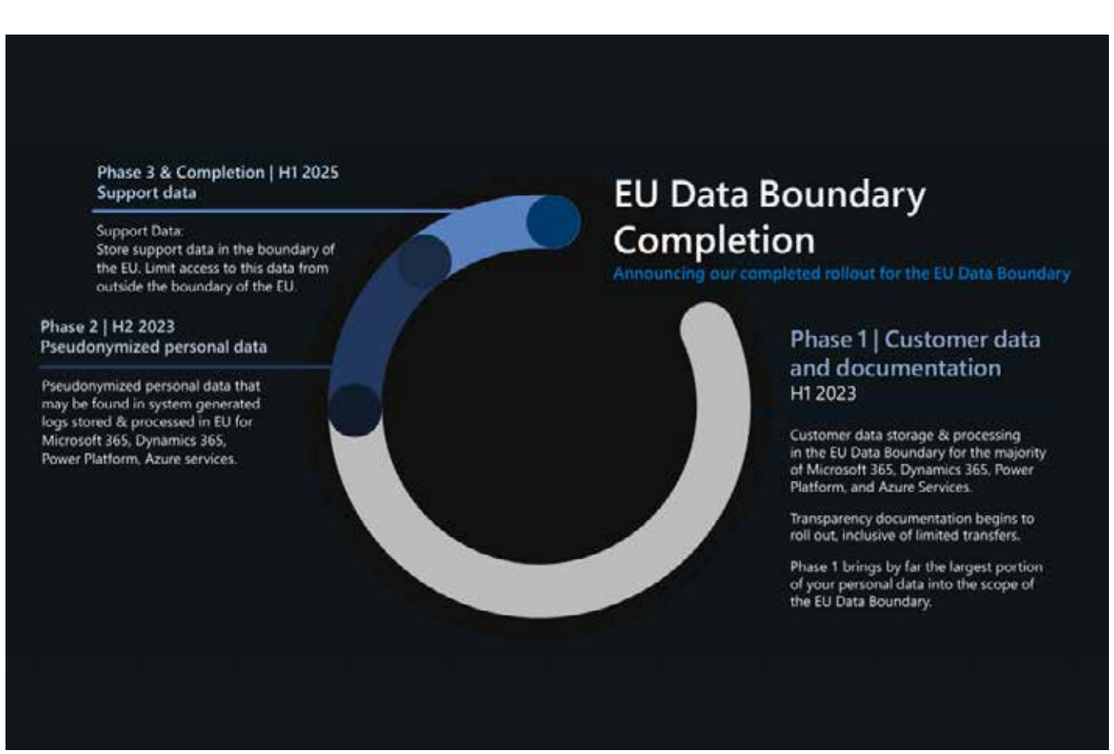


Bild: die Phasen der Bereitstellung der EU Data Boundary. Phase 3 aktiv seit Feb 2025 (empowering-europe-microsofts-eu-data-boundary-roadmap-and-compliance-milestones_20256-02-26.pdf)

Bemerkung:

Dies zeigt einmal mehr, dass Microsoft die EU und auch Deutschland verstanden hat: Kein anderer Anbieter hat diesen Technologiesprung gewagt. Aber Achtung, der sogenannte Tenant muss von Anfang an in der EUDB angelegt werden, ein Nachkonfigurieren ist nicht möglich. Möchten Sie diese als bestehender Cloud-Kunde dennoch nutzen, kann alternativ ein neuer Tenant angelegt und bestehende Subscriptions können migriert werden.

Durch die EU Data Boundary können Kunden ihre Daten mit größerer Transparenz und Kontrolle verwalten. Dies betrifft zentrale Cloud-Dienste wie Microsoft 365, Dynamics 365, Power Platform und die meisten Azure-Dienste. Zudem werden technische Support-Daten, die für professionelle Dienstleistungen relevant sind, ebenfalls innerhalb der EU und EFTA gespeichert (Microsoft – Produktbedingungen).

Die Einführung dieser Datenregion zeigt Microsofts langjähriges Engagement für Datenschutz und Datensicherheit in Europa. Aus meiner Perspektive schafft dieses **Commitment** Vertrauen bei Unternehmen und öffentlichen Einrichtungen, die ihre sensiblen Daten innerhalb europäischer Grenzen verwalten möchten.

Die EU Data Boundary ist somit nicht nur eine technische Lösung, sondern auch ein klares Bekenntnis zur Einhaltung europäischer Standards und zur Stärkung der digitalen Souveränität in Europa.

Um welche Arten von Daten geht es genau?

1

Kundendaten

Wie in den Microsoft-Produktbedingungen definiert, sind Kundendaten alle Daten, einschließlich aller Text-, Ton-, Video- oder Bilddateien und Software, die Microsoft durch die Nutzung des Onlinediensts oder im Auftrag des Kunden zur Verfügung gestellt werden. Kundendaten enthalten keine Professional Services-Daten. Aus Gründen der Übersichtlichkeit enthalten die Kundendaten auch keine Informationen, die zum Konfigurieren von Ressourcen in den Onlinediensten verwendet werden, z. B. technische Einstellungen und Ressourcennamen.

2

Personenbezogene Daten in vom System generierten Protokollen

Microsofts Onlinedienste erstellen im Rahmen des regulären Betriebs systemgenerierte Protokolle. Diese Protokolle zeichnen die Systemaktivität im Laufe der Zeit kontinuierlich auf, damit Microsoft überwachen kann, ob die Systeme wie erwartet funktionieren. Die Speicherung und Verarbeitung von Protokollen ist unerlässlich, um betriebsbezogene Probleme, Richtlinienverstöße und betrügerische Aktivitäten zu identifizieren und darauf zu reagieren.

Beispiele für vom System generierte Protokolle, die personenbezogene Daten enthalten können, sind:

- Produkt- und Dienstnutzungsdaten, wie Aktivitätsprotokolle von Nutzer:innen
- Daten, die speziell durch die Interaktion von Nutzer:innen mit anderen Systemen generiert werden

3

Pseudonymisierung in vom System generierten Protokollen

Microsoft verlangt, dass alle personenbezogenen Daten in vom System generierten Protokollen pseudonymisiert werden. Pseudonymisierung im Sinne von Art. 4 Abs. 5 DSGVO ist die Verarbeitung personenbezogener Daten, sodass sie ohne weitere Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können. Mit anderen Worten: personenbezogene Informationen innerhalb eines Datensatzes werden durch eine oder mehrere künstliche Kennungen oder Pseudonyme ersetzt, wodurch die Identität der betroffenen Person geschützt wird.

Microsoft verwendet verschiedene Techniken, um personenbezogene Daten in vom System generierten Protokollen zu pseudonymisieren, einschließlich Verschlüsselung, Maskierung, Tokenisierung und Unschärfe von Daten.

Unabhängig von der spezifischen Methode der Pseudonymisierung schützt dies die Privatsphäre der Nutzer:innern, indem autorisierte Microsoft-Mitarbeitende ihre Arbeit mithilfe von Protokollen ausführen können, die nur pseudonymisierte personenbezogene Daten enthalten. Dies ermöglicht es, die Qualität, Sicherheit und Zuverlässigkeit der Onlinedienste zu gewährleisten, ohne Nutzer:innen zu identifizieren. So können DevOps-Mitarbeitende beispielsweise das Ausmaß eines Problems regionsübergreifend identifizieren, einschließlich der Anzahl betroffener Nutzer:innen in einer bestimmten Region. Weitere Informationen zum Microsoft DevOps-Modell finden Sie unter Remotezugriff auf Daten, die in der EU-Datengrenze gespeichert und verarbeitet werden.

Microsoft unternimmt mehrere Schritte, um den Zugriff auf und die Verwendung von systemgenerierten Protokollen zu beschränken:

- Datenminimierung durch Implementierung von Aufbewahrungsrichtlinien, die für jeden Protokolltyp auf die mindeste Aufbewahrungszeit festgelegt sind,
- regelmäßige Überprüfungen und Bereinigen von vom System generierten Protokollen, um Fehler oder Nichtkonformität von Richtlinien zu erkennen,
- eingeschränkte Verwendung von vom System generierten Protokollen ausschließlich für Zwecke im Zusammenhang mit Dienstvorgängen, und
- Richtlinien, die Zugriffssteuerungen erfordern, die die Aktivierung oder Neuidentifizierung personenbezogener Daten so einschränken, dass sie in ihre ursprüngliche Form zurückgesendet werden.

4

Professional Services-Daten

Professional Services Daten sind alle Daten (z.B. Texte, Ton-, Video- oder Bilddateien, Software), die Microsoft

1. direkt vom Kunden erhält,
2. auf die Microsoft im Auftrag des Kunden zugreifen darf (z. B. genehmigter Zugriff via Lockbox),
3. die Microsoft anderweitig in der Zusammenarbeit vom Kunden weiterverarbeitet.

Konfiguration von Diensten für die Verwendung in der EU-Datengrenze

Für EU Data Boundary Services werden Kundendaten und pseudonymisierte personenbezogene Daten gespeichert und verarbeitet und Professional Services-Daten werden im Ruhezustand in Rechenzentren in Ländern der EU oder EFTA gespeichert.

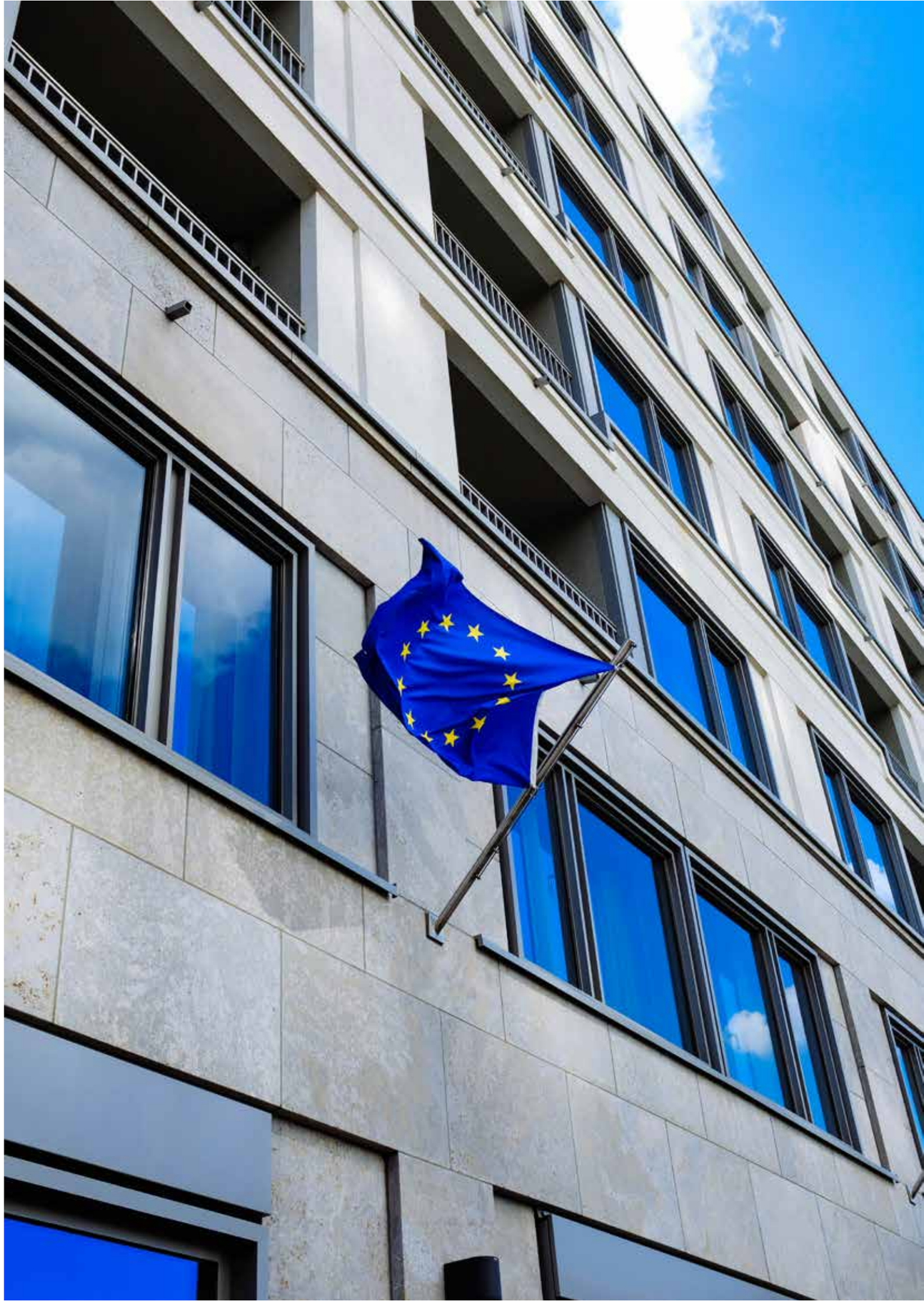
In einigen Fällen können Kunden die EU-Bereitstellungsregion für Kundendaten direkt auswählen, in anderen wird der Standort automatisch basierend auf dem Kundenstandort, der Rechnungsadresse oder einer Kundenentscheidung, dass sich seine Umgebung in der EU-Datengrenze befindet, zugewiesen.

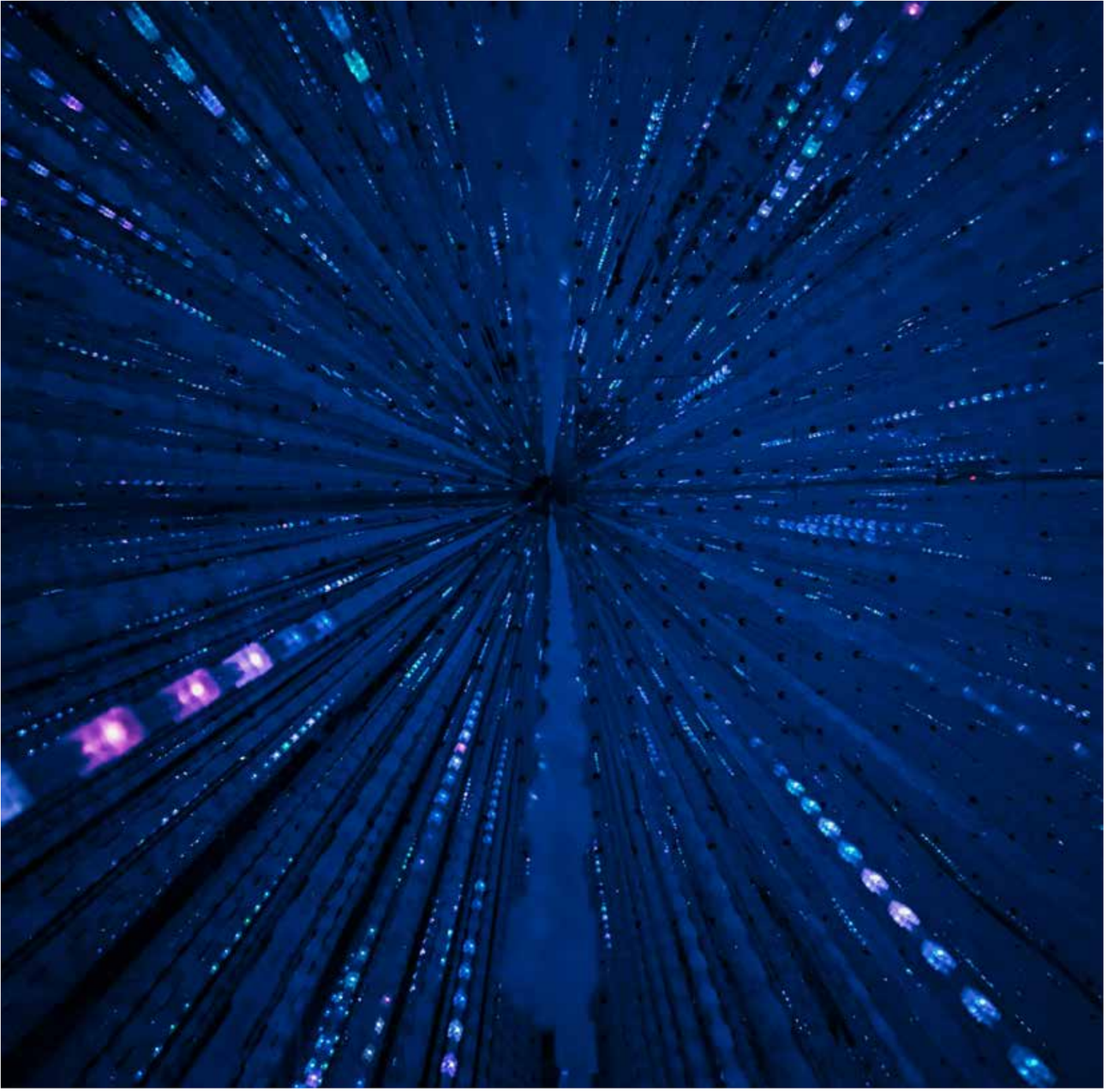
Für **Azure** fallen regionale Dienste, die ein Kunde in einer EU-Datenbegrenzungsregion bereitstellt, in den Geltungsbereich der EU-Datengrenze. Weitere Informationen, einschließlich Details zu den Azure-Regionen in der EU und EFTA, finden Sie unter Data Residency in Azure. Informationen zum Konfigurieren der einzelnen Dienste für nicht regionale Azure-Dienste für die EU-Datengrenze finden Sie unter Konfigurieren nicht regionaler Azure-Dienste für die EU-Datengrenze.

Um Professional Services-Daten in der EU-Datengrenze für Azure zu speichern, müssen Kunden den Azure Resource Manager an die EU-Datengrenze konfigurieren. Weitere Informationen finden Sie unter Konfigurieren nicht regionaler Azure-Dienste für die EU-Datengrenze.

Bei **Dynamics 365 und Power Platform** wird der geografische Bereich, in dem der Dienstmandant eines Kunden gehostet wird, durch die Abrechnungsadresse bestimmt. Kunden können ihre Dienste so konfigurieren, dass sie für die EU-Datengrenze gelten, indem sie ihren Mandanten und alle vwwDynamics 365- und Power Platform-Umgebungen in einem geografischen Raum in der EU-Datengrenze bereitstellen. Weitere Informationen finden Sie unter Internationale Verfügbarkeit von Dynamics 365 und Erstellen und Verwalten von Umgebungen im Power Platform Admin Center.

Für **Microsoft 365** gilt für Kunden mit einem Registrierungsstandort in einem Land oder einer Region in der EU oder EFTA die EU-Datengrenze. Kunden, die Multi-Geo-Funktionen erworben haben, fallen jedoch nicht in den Geltungsbereich der EU-Datengrenze, auch wenn ihr Mandant als in einem Land oder einer Region in der EU oder EFTA aufgeführt ist. Kunden können das Land oder die Region ihres Mandanten im Microsoft 365 Admin Center überprüfen.





Microsoft Sovereign Public Cloud

Einführung

Definition und Ziele:

Microsoft Sovereign Public Cloud ist eine speziell entwickelte Cloud-Lösung, die darauf abzielt, Unternehmen jeglicher Industriezweige, Regierungen und öffentliche Institutionen dabei zu unterstützen, ihre Workloads in der Microsoft Cloud zu erstellen und zu transformieren, während sie die lokalen Datenschutz- und Sicherheitsanforderungen erfüllen. Diese Lösung bietet eine Kombination aus Datenresidenz, erweiterten Sicherheitsfunktionen und Compliance-Kontrollen, um sicherzustellen, dass sensible Daten innerhalb der regionalen Grenzen bleiben und den gesetzlichen Vorschriften entsprechen.

Die Hauptziele sind:

Sicherstellung der Datenhoheit: Gewährleistung, dass Daten innerhalb der geografischen Grenzen eines Landes gespeichert und verarbeitet werden, um die Souveränität über die Daten zu bewahren.

Erfüllung lokaler Compliance-Anforderungen: Unterstützung bei der Einhaltung lokaler Datenschutzgesetze und -vorschriften durch vorgefertigte Compliance-Pakete und Richtlinien.

Förderung der digitalen Transformation: Ermöglichung der Modernisierung und Verbesserung wirtschaftlicher und öffentlicher Dienstleistungen durch den Einsatz moderner Cloud-Technologien.

Geschichte und Entwicklung

Die Entwicklung von Microsoft Sovereign Public Cloud ist eng mit den wachsenden Anforderungen an Datenschutz und digitale Souveränität verbunden. In den letzten Jahren haben viele Länder strengere Datenschutzgesetze eingeführt, die die Speicherung und Verarbeitung von Daten innerhalb ihrer Grenzen vorschreiben. Diese Gesetze zielen darauf ab, die Kontrolle über sensible Daten zu behalten und die Privatsphäre der Bürger:innen zu schützen.

Microsoft hat auf diese Anforderungen reagiert, indem es eine Cloud-Lösung entwickelt hat, die speziell auf diese Bedürfnisse zugeschnitten sind. Die Einführung der Microsoft Sovereign Public Cloud in 2022 markiert einen wichtigen Schritt in der Entwicklung von Cloud-Technologien, die den Anforderungen an Datenschutz, Sicherheit und Compliance gerecht werden. Im Juni 2025 geht Microsoft noch einen Schritt weiter und kündigt eine erweiterte Form der Sovereign Public Cloud mit Data Guardian, External Key Management und Microsoft 365 Local und Azure Local an.

Bedeutung der digitalen Souveränität

Digitale Souveränität bezieht sich auf die Fähigkeit eines Unternehmens bzw. eines Staates, die Kontrolle über seine digitalen Ressourcen und Daten zu behalten. Dies umfasst die Speicherung, Verarbeitung und Verwaltung von Daten innerhalb der geografischen Grenzen des Landes sowie die Einhaltung lokaler Datenschutzgesetze und -vorschriften.

Die Bedeutung der digitalen Souveränität hat in den letzten Jahren zugenommen, da immer mehr Länder erkennen, wie wichtig es ist, die Kontrolle über ihre Daten zu behalten.

Dies ist besonders relevant für Regierungen und öffentliche Institutionen sowie Unternehmen, die mit hochsensiblen Daten arbeiten, und sicherstellen müssen, dass diese Daten vor unbefugtem Zugriff und Sicherheitsverletzungen geschützt sind. Dies betrifft z.B. Banken, Versicherungen oder Krankenhäuser.

Aber natürlich wollen und müssen auch Unternehmen aus Produktion, Handel, R&D usw. dies ebenso realisieren.

Herausforderungen und Lösungen in diesem Zusammenhang

Die Einführung von Cloud-Technologien bringt eine Reihe von Herausforderungen mit sich, darunter:

Datenschutz und Sicherheit

Sicherstellung, dass sensible Daten vor unbefugtem Zugriff und Sicherheitsverletzungen geschützt sind.

Compliance

Einhaltung lokaler Datenschutzgesetze und -vorschriften.

Transparenz und Kontrolle

Gewährleistung der Transparenz und Kontrolle über die Cloud-Operationen.

Microsoft Sovereign Public Cloud bietet Lösungen für diese Herausforderungen, indem es erweiterte Sicherheitsfunktionen, Compliance-Kontrollen und Mechanismen zur Überwachung und Kontrolle der Cloud-Operationen bereitstellt. Diese Lösung ermöglicht es, die Vorteile der Cloud-Technologie zu nutzen, ohne Kompromisse bei Sicherheit, Datenschutz und Compliance einzugehen.

Hauptmerkmale und Vorteile

1

Datenresidenz und Souveränität

Datenresidenz bezieht sich auf die physische Speicherung und Verarbeitung von Daten innerhalb bestimmter geografischer Grenzen.

Microsoft Sovereign Public Cloud bietet die Möglichkeit, Daten in regionalen Rechenzentren zu speichern und zu verarbeiten. Dies gewährleistet, dass die Daten den lokalen Gesetzen und Vorschriften entsprechen und nicht außerhalb der festgelegten geografischen Grenzen gelangen. Diese Funktion ist besonders wichtig für Länder mit strengen Datenschutzgesetzen, die die Speicherung und Verarbeitung von Daten innerhalb ihrer Grenzen vorschreiben.

2

Sicherheits- und Compliance-Kontrollen

Die Sicherheit und der Schutz sensibler Daten sind von größter Bedeutung für Regierungen und öffentliche Institutionen. Microsoft Sovereign Public Cloud bietet erweiterte Sicherheitsfunktionen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten. Zu den wichtigsten Sicherheitsfunktionen gehören:

Verschlüsselung: Daten werden sowohl im Ruhezustand als auch während der Übertragung verschlüsselt, um sie vor unbefugtem Zugriff zu schützen ***(Tipp: Schenken Sie dem Thema „Data at Rest“, „Data in Transit“ und „Data in Use“ besondere Aufmerksamkeit).***

Zugriffskontrollen: Strenge Zugriffskontrollen stellen sicher, dass nur autorisierte Personen auf die Daten zugreifen können (Tipp: Schauen Sie sich auch das Thema LockBox an, es ist Teil der M365 E5 Lizenz).

Überwachungsmechanismen: Kontinuierliche Überwachung und Protokollierung von Aktivitäten helfen dabei, verdächtige Aktivitäten zu erkennen und zu verhindern. Zusätzlich zu den Sicherheitsfunktionen unterstützt Microsoft Sovereign Public Cloud die Einhaltung gesetzlicher Vorschriften und lokaler Richtlinien durch vorgefertigte Compliance-Pakete. Diese Pakete enthalten Richtlinien und Best Practices.

Transparenz und Governance: Transparenz und Kontrolle über die Cloud-Operationen sind entscheidend, um die Einhaltung von Sicherheits- und Betriebsstandards zu gewährleisten. Microsoft Sovereign Public Cloud bietet Mechanismen zur Überwachung und Steuerung der Cloud-Umgebung, darunter:

- **Erweiterte Audit-Rechte:** Kunden erhalten erweiterte Rechte zur Überprüfung und Überwachung der Cloud-Operationen, um sicherzustellen, dass alle Aktivitäten den Sicherheits- und Compliance-Anforderungen entsprechen. Die Freischaltung des Transparency Logs muss bei Microsoft beantragt werden.

- **Governance-Tools:** Tools zur Verwaltung und Steuerung der Cloud-Ressourcen helfen dabei, die Einhaltung von Richtlinien und Standards zu gewährleisten.

Diese Funktionen ermöglichen es, eine umfassende Transparenz und Kontrolle über Ihre Cloud-Umgebung zu behalten und sicherzustellen, dass alle Aktivitäten den festgelegten Standards entsprechen.

3

Innovationsförderung

Die Nutzung der Cloud-Technologie bietet Unternehmen, Regierungen und öffentlichen Institutionen die Möglichkeit, schneller zu innovieren und ihre Dienstleistungen zu verbessern. Microsoft Sovereign Public Cloud unterstützt moderne Technologien, die ohne die Cloud nicht möglich wären, darunter:

Künstliche Intelligenz (KI): KI-Technologien können genutzt werden, um Prozesse zu automatisieren, Datenanalysen durchzuführen und bessere Entscheidungen zu treffen.
Tipp: Prüfen Sie Verträge der Hyperscaler im Hinblick auf KI. Insbesondere zu den Fragen: Wem gehören die Daten und wer darf diese Daten verwenden, sei es auch nur zu analytischen Zwecken. Hier ist aus meiner Sicht wieder Microsoft der Platzhirsch in puncto Transparenz.
An dieser Stelle auch der Verweis auf die ethischen Werte verweisen, denen sich Microsoft zum Thema KI verpflichtet hat: [Fördern verantwortungsvoller KI-Praktiken | Microsoft KI]

Blockchain: Blockchain-Technologien bieten sichere und transparente Möglichkeiten zur Verwaltung von Transaktionen und Daten.

Digitale Identität: Lösungen für digitale Identität ermöglichen es, sichere und vertrauenswürdige digitale Identitäten für Bürger:innen und Mitarbeitende zu erstellen und zu verwalten. Durch die Nutzung dieser Technologien können öffentliche Institutionen ihre Dienstleistungen modernisieren, die Effizienz verbessern und die User Experience für Bürger:innen und Mitarbeitende optimieren.

Technische Details und Architektur

Cloud Guardrails

Cloud Guardrails sind codierte Architektur- und Workload-Vorlagen, die sicherstellen, dass alle Cloud-Ressourcen den lokalen Vorschriften und Sicherheitsstandards entsprechen. Diese Guardrails bieten eine strukturierte und standardisierte Methode zur Implementierung und Verwaltung von Cloud-Ressourcen, um die Einhaltung von Richtlinien und Best Practices zu gewährleisten.

Die Hauptfunktionen der Cloud Guardrails umfassen:

Automatisierte Richtlinien: Vordefinierte Richtlinien, die automatisch auf Cloud-Ressourcen angewendet werden, um sicherzustellen, dass sie den Sicherheits- und Compliance-Anforderungen entsprechen.

Überwachung und Berichterstattung: Kontinuierliche Überwachung der Cloud-Ressourcen und Berichterstattung über deren Einhaltung der Richtlinien.

Anpassungsfähigkeit: Die Möglichkeit, die Guardrails an spezifische Anforderungen und Vorschriften anzupassen, um eine maßgeschneiderte Lösung für jede Organisation zu bieten.

Hardware-basierte Verschlüsselung (Managed HSMs)

Hardware-basierte Verschlüsselung bietet zusätzlichen Schutz für sensible Daten, indem sie Verschlüsselungskontrollen auf Hardware-Ebene implementiert. Diese Technologie stellt sicher, dass Daten sowohl im Ruhezustand, als auch während der Übertragung vor unbefugtem Zugriff geschützt sind.

Die Vorteile der hardware-basierten Verschlüsselung umfassen:

Erhöhte Sicherheit: Schutz vor physischen Angriffen auf die Hardware, die die Daten speichert.

Leistungsoptimierung: Effiziente Verschlüsselung, die die Leistung der Cloud-Ressourcen nicht beeinträchtigt.

Vertraulichkeit: Gewährleistung der Vertraulichkeit sensibler Daten durch starke Verschlüsselungsalgorithmen.

Azure Policy Initiatives

Azure Policy Initiatives sind lokalisierte Richtlinien und Tools, die helfen, die Einhaltung von Vorschriften zu überwachen und zu gewährleisten. Diese Initiativen bieten eine strukturierte Methode zur Implementierung und Verwaltung von Richtlinien, die speziell auf die Anforderungen des öffentlichen Sektors zugeschnitten sind.

Die Hauptfunktionen der Azure Policy Initiatives umfassen:

Richtliniendefinition: Erstellung und Verwaltung von Richtlinien, die den lokalen Vorschriften und Best Practices entsprechen.

Compliance-Überwachung: Kontinuierliche Über-wachung der Cloud-Ressourcen, umsicherzustellen, dass sie den definierten Richtlinien entsprechen.

Berichterstattung: Detaillierte Berichte über die Einhaltung der Richtlinien und Identifizierung von Abweichungen.

Architektur und Design

Die Architektur von Microsoft Sovereign Public Cloud ist darauf ausgelegt, die spezifischen Anforderungen von Regierungen und öffentlichen Institutionen zu erfüllen. Sie umfasst eine Reihe von Komponenten und Designprinzipien, die eine sichere und effiziente Nutzung der Cloud-Ressourcen ermöglichen.

Die Hauptkomponenten der Architektur umfassen:

Regionale Rechenzentren: Bereitstellung von Cloud-Ressourcen in regionalen Rechenzentren, um die Datenresidenz und Souveränität zu gewährleisten.

Sicherheits- und Compliance-Module: Integration von Sicherheits- und Compliance-Modulen, die die Einhaltung lokaler Vorschriften und Best Practices unterstützen.

Governance-Tools: Bereitstellung von Tools zur Verwaltung und Steuerung der Cloud-Ressourcen, um eine umfassende Transparenz und Kontrolle zu gewährleisten.

Die Designprinzipien umfassen:

Modularität: Die Möglichkeit, die Architektur an spezifische Anforderungen und Vorschriften anzupassen.

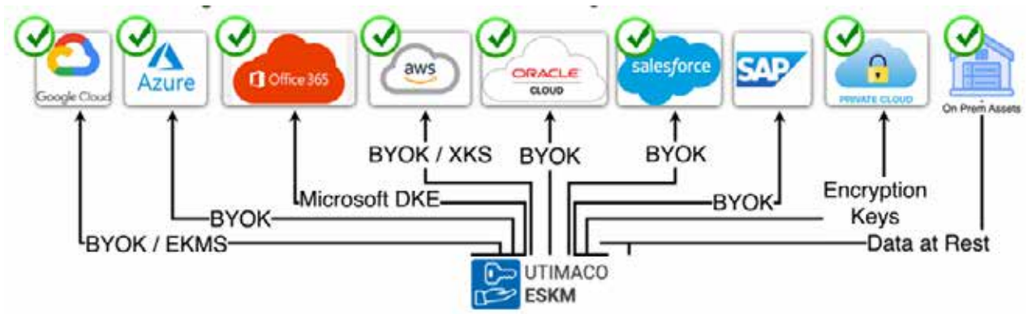
Skalierbarkeit: Die Option, die Cloud-Ressourcen bei Bedarf zu skalieren, um den wachsenden Anforderungen gerecht zu werden.

Effizienz: Optimierung der Leistung und Effizienz der Cloud-Ressourcen, um eine kosteneffektive Nutzung zu gewährleisten.

Bemerkung:

Sollte diese HSM Verschlüsselung, aus welchen Gründen auch immer, nicht den eigenen Sicherheitsbedarf und Vertrauensbedürfnis erfüllen, können Sie sich die Sicherheitslösung der Firma Utimaco aus Aachen genauer ansehen, die zwei Ansätze bereit stellt: Bring your OwnKey und Hold your OwnKey.

Utimaco ist Partner der novaCapta und bietet „Deutsche Ingenieurskunst“ seit über 40 Jahren. Die Partnerschaft bietet Kunden die einzigartige Möglichkeit die Utimaco- mit den Microsoft- Technologien zu kombinieren. Das Interessante ist, dass Utimaco der einzige zugelassene HSM Provider des BSIs (Stand 2025) ist und sich die Lösungen optimal in Public Clouds integrieren lassen.



Hauptbestandeile dieser Lösung sind die uTrust Anchor Plattform (HSMs), auf der vereinfacht gesagt „Schlüssel gespeichert werden”, sowie der ESKM (Enterprise Secure Key Manager), der für das gesamte Management der Schlüssel verantwortlich ist (u.a. Weitergabe an Azure KeyVault, Attribute setzten, überprüfen).

Letzterer kann als virtuelle Instanz auf der HSM mit betrieben werden, wobei eine VM innerhalb von Microsoft Azure aus meiner Sicht die schönere und bessere Variante darstellt.

Folgende Komponenten in Azure bzw. in der M365-Anbindung sind notwendig:

- Azure Landing Zone (ALZ), bzw. Sovereignty Landing Zone
- Azure Virtuelle Maschine (VMs)
- Microsoft Azure Key Vault
- Azure Loadbalancer
- Azure Site-to-Site VPN Verbindung
- Azure virtual Network (vNet)
- Microsoft Purview und Sentinel (beides als Empfehlung)

Im Rahmen der Ankündigung zu External Key Management zur Erweiterung von Azure Managed HSM durch Microsoft CEO Satya Nadella im Juni 2025, wird Utimaco als einer der wenigen HSM-Hersteller genannt, mit denen Microsoft bei der Entwicklung zusammenarbeitet.

Bemerkung für sehr sensible Daten „in use“ (diese sollten ausgewählt behandelt werden):

Wenn Sie bestimmte Workloads während der Nutzung noch besonders absichern wollen, empfehle ich „Azure Confidential Computing“ näher in Betracht zu ziehen.

1. Schützen Sie Daten während der Verwendung:
Es verschlüsselt Daten im Arbeitsspeicher in hardwarebasierten vertrauenswürdigen Ausführungsumgebungen und verarbeitet sie erst, nachdem die Cloudumgebung überprüft wurde, wodurch der Datenzugriff durch Cloudanbieter, Administrator:innen und Benutzer:innen verhindert wird.

2. KI Erkenntnisse vertraulich teilen
Kombinieren Sie Datasets vertraulich, ohne Ihre Daten für andere mitwirkende Organisationen verfügbar zu machen (dies ist besonders relevant, wenn befreundete Unternehmen von Analyse-Daten profitieren wollen, die Originaldaten aber nicht direkt teilen wollen). Verschlüsselte Daten werden dabei in eine Secure Enclave auf einem virtuellen Computer hochgeladen und es werden Algorithmen auf Datasets über mehrere Quellen angewendet.

3. Kontrolle über eigene Daten behalten
Sie können die Hardware und Software angeben, die Zugriff auf Ihre Daten und Ihren Code haben sollen. Sie behalten die Kontrolle über Ihre geschützten Informationen, damit Sie behördliche Vorschriften und Compliance-Anforderungen erfüllen können.

Ebenso passen Sie Ihren Confidential Computing-Pfad mithilfe von Tools und Lösungen an, die in Azure, in Open-Source-Frameworks und von unabhängigen Softwareanbieterpartnern erstellt wurden.

Sprechen Sie uns gerne dazu an, da Azure Confidential Computing nicht über alle Komponenten in Azure verfügbar ist.

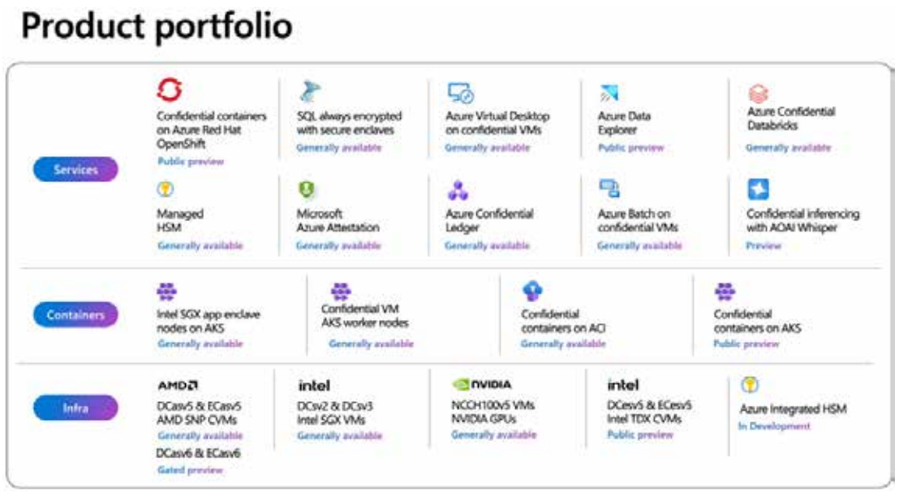


Bild: Ein Auszug aus Diensten (Stand Mitte 2025)

Unterschiede zu Azure Landing Zones

Zweck und Zielgruppe

Microsoft Sovereign Public Cloud und **Azure Landing Zones** sind beide darauf ausgelegt, Organisationen bei der Nutzung der Azure Cloud zu unterstützen, jedoch mit unterschiedlichen Schwerpunkten und Zielgruppen.

Microsoft Sovereign Public Cloud:

Diese Lösung ist speziell entwickelt, um strenge Anforderungen an Datenschutz, Sicherheit und Compliance zu realisieren. Sie zielt darauf ab, die digitale Souveränität zu gewährleisten, indem sie sicherstellt, dass Daten innerhalb der geografischen Grenzen eines Landes gespeichert und verarbeitet werden. Die Hauptzielgruppe sind staatliche Stellen, die ihre sensiblen Daten schützen und gleichzeitig die Vorteile der Cloud-Technologie nutzen möchten.

Azure Landing Zones:

Diese vorkonfigurierten Umgebungen sind für eine breitere Zielgruppe von Unternehmen und Organisationen konzipiert, die ihre Workloads in der Azure Cloud hosten und skalieren möchten. Azure Landing Zones bieten eine modulare und skalierbare Architektur, die es Unternehmen ermöglicht, ihre Cloud-Ressourcen effizient zu verwalten und zu optimieren.

Architektur und Design

Die Architektur und das Design von Microsoft Sovereign Public Cloud und Azure Landing Zones unterscheiden sich in mehreren Aspekten:

Microsoft Sovereign Public Cloud:

Cloud Guardrails: Codierte Architektur- und Workload-Vorlagen, die sicherstellen, dass alle Cloud-Ressourcen den lokalen Vorschriften und Sicherheitsstandards entsprechen.

Regionale Rechenzentren: Bereitstellung von Cloud-Ressourcen in regionalen Rechenzentren, um die Datenresidenz und Souveränität zu gewährleisten. (*Notiz: Der Irrglaube, dass Microsoft Clouds nur in den USA sind und alle Daten über den „Teich" gehen, ist weiterhin stark verbreitet. Das ist schlichtweg falsch. Allein in Deutschland gibt es zwei Regionen (Frankfurt und Magdeburg), zudem zwei sehr große in den Niederlanden sowie in Irland.)*

Sicherheits- und Compliance-Module: Integration von Sicherheits- und Compliance-Modulen, die speziell auf die Anforderungen des öffentlichen Sektors zugeschnitten sind.

Azure Landing Zones:

Modularität und Skalierbarkeit: Designprinzipien, die eine flexible und skalierbare Implementierung von Cloud-Ressourcen ermöglichen.

Best Practices: Vordefinierte Best Practices und Richtlinien, die eine konsistente Anwendung von Konfigurationen und Kontrollen gewährleisten.

Automatisierung: Einsatz von Automatisierungstools zur effizienten Verwaltung und Optimierung der Cloud-Umgebungen.

Tipp: Erfahren Sie mehr zum Azure Landingzone Ansatz und Angebot der novaCapta

Sicherheits- und Compliance-Funktionen

Sicherheits- und Compliance-Funktionen sind zentrale Aspekte sowohl von Microsoft Sovereign Public Cloud als auch von Azure Landing Zones, jedoch mit unterschiedlichen Schwerpunkten:

Microsoft Sovereign Public Cloud:

Erweiterte Sicherheitsfunktionen: Umfassende Sicherheitsmaßnahmen wie hardwarebasierte Verschlüsselung, strenge Zugriffskontrollen und kontinuierliche Überwachung, um die Vertraulichkeit und Integrität der Daten zu gewährleisten.

Spezifische Compliance-Pakete: Vorbereitete Compliance-Pakete, die speziell auf die gesetzlichen Anforderungen und Richtlinien des öffentlichen Sektors zugeschnitten sind.

Transparenz und Governance: Erweiterte Audit-Rechte und Governance-Tools, die eine umfassende Überwachung und Kontrolle der Cloud-Operationen ermöglichen.

Azure Landing Zones:

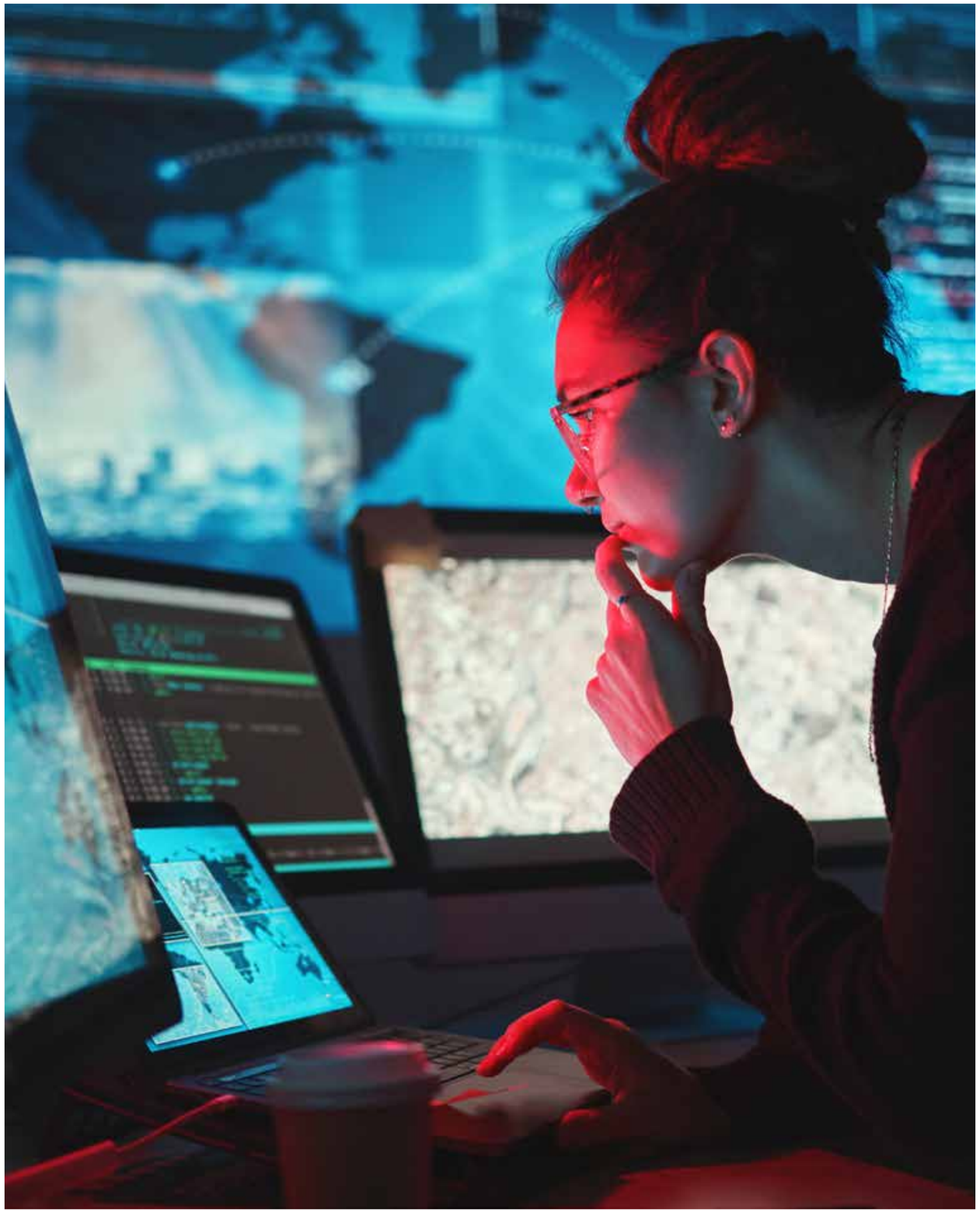
Allgemeine Sicherheits- und Governance-Prinzipien: Sicherheits- und Governance-Prinzipien, die für eine breite Palette von Unternehmensanwendungen geeignet sind.

Richtlinien und Best Practices: Vordefinierte Richtlinien und Best Practices, die eine konsistente Anwendung von Sicherheits- und Compliance-Kontrollen gewährleisten.

Automatisierte Compliance-Überwachung: Tools zur automatisierten Überwachung und Berichterstattung über die Einhaltung von Sicherheits- und Compliance-Anforderungen.

Fazit

Sowohl Microsoft Sovereign Public Cloud als auch Azure Landing Zones zielen darauf ab, Organisationen bei der Nutzung der Azure Cloud zu unterstützen, unterscheiden sie aber in ihren spezifischen Schwerpunkten und Zielgruppen. Microsoft Sovereign Public Cloud ist speziell auf die Bedürfnisse von regulierten Unternehmen, Regierungen und öffentlichen Institutionen zugeschnitten, die strenge Anforderungen an Datenschutz, Sicherheit und Compliance haben.



Implementierung

Schritte zur Implementierung

Die erfolgreiche Implementierung von Microsoft Sovereign Public Cloud erfordert eine sorgfältige Planung und Ausführung. Die wesentlichen Schritte:

1

Bedarfsanalyse und Planung:

Anforderungsdefinition: Identifizierung der spezifischen Anforderungen und Ziele der Organisation, einschließlich Datenschutz, Sicherheit und Compliance.

Ressourcenplanung: Bestimmen der benötigten Ressourcen, einschließlich technischer Infrastruktur, Personal und Budget.

2

Architekturdesign und Konfiguration:

Cloud Guardrails: Implementierung von codierten Architektur- und Workload-Vorlagen, die sicherstellen, dass alle Cloud-Ressourcen den lokalen Vorschriften und Sicherheitsstandards entsprechen.

Regionale Rechenzentren: Auswahl und Konfiguration der regionalen Rechenzentren, um die Datenresidenz und Souveränität zu gewährleisten.

3

Sicherheits- und Compliance-Setup:

Verschlüsselung und Zugriffskontrollen: Implementierung von Verschlüsselungstechnologien und strengen Zugriffskontrollen, um die Vertraulichkeit und Integrität der Daten zu gewährleisten.

Compliance-Pakete: Nutzung vorgefertigter Compliance-Pakete, die speziell auf die gesetzliche Anforderungen und Richtlinien zugeschnitten sind.

4

Migration und Integration:

Datenmigration: Sicherstellung einer sicheren und effizienten Migration bestehender Daten in die Cloud-Umgebung.

Systemintegration: Integration der Cloud-Lösung mit bestehenden Systemen und Anwendungen, um eine nahtlose Zusammenarbeit zu gewährleisten.

5

Überwachung und Optimierung:

Überwachungsmechanismen: Implementierung kontinuierlicher Überwachungs- und Protokollierungsmechanismen, um die Einhaltung von Sicherheits- und Compliance-Anforderungen zu gewährleisten.

Leistungsoptimierung: Regelmäßige Überprüfung und Optimierung der Cloud-Ressourcen, um die Effizienz und Leistung zu maximieren.

Best Practices

Schritte zur Implementierung

Um die Vorteile von Microsoft Sovereign Public Cloud voll auszuschöpfen, sollten Sie folgende Best Practices befolgen:

1. Sicherheitsbewusstsein fördern:

- **Schulungen und Sensibilisierung:** Regelmäßige Schulungen und Sensibilisierungsprogramme für Mitarbeitende, um das Bewusstsein für Sicherheits- und Datenschutzbestimmungen zu erhöhen.
- **Sicherheitsrichtlinien:** Entwicklung und Implementierung klarer Sicherheitsrichtlinien, die von allen Mitarbeitenden befolgt werden müssen.

2. Compliance kontinuierlich überwachen:

- **Regelmäßige Audits:** Durchführung regelmäßiger Audits und Überprüfungen, um sicherzustellen, dass alle Cloud-Ressourcen den gesetzlichen Anforderungen und Richtlinien entsprechen.
- **Compliance-Tools:** Nutzung von Compliance-Tools und -Technologien, um die Einhaltung von Vorschriften kontinuierlich zu überwachen und zu gewährleisten.

3. Transparenz und Governance sicherstellen:

- **Governance-Frameworks:** Implementierung von Governance-Frameworks, die eine umfassende Überwachung und Kontrolle der Cloud-Operationen ermöglichen.
- **Transparenzberichte:** Erstellung regelmäßiger Transparenzberichte, die die Einhaltung von Sicherheits- und Betriebsstandards dokumentieren.

4. Innovationen fördern:

- **Technologie-Updates:** Regelmäßige Aktualisierung der Cloud-Technologien, um von den neuesten Innovationen und Verbesserungen zu profitieren.
- **Pilotprojekte:** Durchführung von Pilotprojekten, um neue Technologien und Ansätze zu testen und deren Nutzen zu bewerten.

5. Zusammenarbeit und Partnerschaften:

- **Stakeholder-Engagement:** Einbindung aller relevanten Stakeholder in den Implementierungsprozess, um deren Anforderungen und Bedenken zu berücksichtigen *(Vergessen Sie hier auch nicht den Betriebsrat, falls vorhanden. Eine frühzeitige Einbindung schafft Vertrauen!)*
- **Partnerschaften:** Aufbau von Partnerschaften mit Technologieanbietern und anderen Institutionen bzw. Unternehmen, um Best Practices auszutauschen und voneinander zu lernen *(Sprechen sie mich gerne an, ob es hierzu schon etwas gibt).*

Ausblick: Zukunftsaussichten und Weiterentwicklung

Technologische Trends

Die Zukunft der digitalen Souveränität und Cloud-Technologien wird von mehreren wichtigen Trends geprägt, die die Art und Weise, wie Regierungen, öffentliche Institutionen und Unternehmen ihre Daten verwalten und nutzen, verändern werden:

1

Künstliche Intelligenz und maschinelles Lernen:

Automatisierung: KI und maschinelles Lernen werden zunehmend zur Automatisierung von Prozessen und zur Verbesserung der Effizienz eingesetzt.

Datenanalyse: Fortschritte in der Datenanalyse ermöglichen es, große Datenmengen zu verarbeiten und wertvolle Erkenntnisse zu gewinnen. Dies kann dazu beitragen, die Qualität der Dienstleistungen zu verbessern und gezielte Maßnahmen zu ergreifen.

Kundentreue: Gerne möchte ich hier auch schon den Punkt Kundentreue und Kundenbindung ansprechen. Es gibt mittlerweile deutsche Unternehmen, die sich auf Basis der Cloud spezialisiert haben, sogenannte ContactCenter zur revolutionieren mit Hilfe von KI. Lange Wartezeiten am Telefon, nervige Abfragen, ob man auch derjenige ist der gerade anruft uvm. gehören der Vergangenheit an.

2

Internet der Dinge (IoT):

Vernetzte Geräte: IoT-Technologien ermöglichen die Vernetzung von Geräten und Systemen, um Daten in Echtzeit zu sammeln und zu analysieren. Effizienz von Infrastruktur und Dienstleistungen werden verbessert.

Smart Cities: IoT spielt eine zentrale Rolle bei der Entwicklung von Smart Cities, die durch vernetzte Technologien effizienter und nachhaltiger werden.

3

Quantencomputing:

Rechenleistung: Quantencomputing bietet eine enorme Rechenleistung, die komplexe Berechnungen und Datenanalysen ermöglicht.

Sicherheit: Fortschritte im Quantencomputing können auch die Sicherheit von Verschlüsselungstechnologien verbessern und neue Möglichkeiten zur Sicherung sensibler Daten bieten.

Die souveräne Landschaft von Microsoft Azure: Wahlmöglichkeiten für Ihre Workload-Platzierung

	Sovereign Public Cloud	National Partner Clouds	Sovereign Private Cloud
	Branchenführende Souveränitätskontrollen in der Public Cloud (z. B. EU-Datengrenze, EU-basierter Support), Verschlüsselung E-2-E	Höchste Souveränitätsstandards nach BSI Cloud Platform Requirements (CPR) Deutschland – Delos Cloud	Zusätzliche selbst gehostete Option für spezifische Souveränitäts-anforderungen
	EU/ EFTA	National	Lokal
	Jeder/ Reg. Branchen	Government / Kritis	Jeder
Skalierbarkeit, Innovation und Resilienz	★★★	★★	★

Bild: Zusammenfassung einiger Sovereign Public Cloud Features

Fazit

Die Zukunft der digitalen Souveränität und Cloud-Technologien ist vielversprechend und bietet zahlreiche Möglichkeiten für Wirtschaft, Regierungen und öffentliche Institutionen, ihre Dienstleistungen zu verbessern und die Effizienz zu steigern. Microsoft Sovereign Public Cloud spielt eine zentrale Rolle bei der Unterstützung dieser Entwicklungen, indem es sichere, transparente und innovative Lösungen bietet, die den Anforderungen aller Kunden gerecht werden.

Durch die kontinuierliche Investition in Forschung und Entwicklung, die Förderung von Partnerschaften und die Umsetzung nachhaltiger Praktiken setzt Microsoft neue Maßstäbe für die Cloud-Technologie und trägt dazu bei, eine vertrauenswürdige und zukunftsfähige digitale Infrastruktur zu schaffen.

Die German Angst vor Microsoft als Anbieter und vor Cloud-Technologien insgesamt sowie KI-Nutzung ist also weitestgehend unbegründet oder kann mit der richtigen Handhabe der zur Verfügung stehenden Mittel deutlich reduziert werden.

Gerne beraten meine novaCapta-Kolleg:innen und ich Sie ausführlich zu den für Sie passenden Cloud-Lösungen, Sicherheitskonzepten und KI-Strategien und Technologien.

novaCapta

Ihr Microsoft Premium Partner

Kontaktieren Sie uns!

Bei Fragen zu unseren Themen sind wir gerne für Sie da und finden gemeinsam mit Ihnen die beste Auswahl aus den Microsoft Bausteinen

DE

novaCapta GmbH
Im Mediapark 5c
50670 Köln

T +49 (0)221 58919 343
M info@novacapta.com
W www.novacapta.de

CH

novaCapta Schweiz AG
Theaterstrasse 17
8400 Winterthur

T +41 (0)41 392 20 00
M info.schweiz@novacapta.com
W www.novacapta.ch