

Public in the Air Microsoft und Ai

Möglichkeiten für den Public Sektor

Konstantin Gratschow

Fokus Manager Microsoft

ADN Distribution GmbH



ADN

Microsoft for Public Sektor



BSI



DSGVO



Microsoft Cloud
Services



DELOS Cloud

BSI

Im Jahr 2016 erstellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Anforderungskatalog „Cloud Computing Compliance Controls Catalog“ (C5).

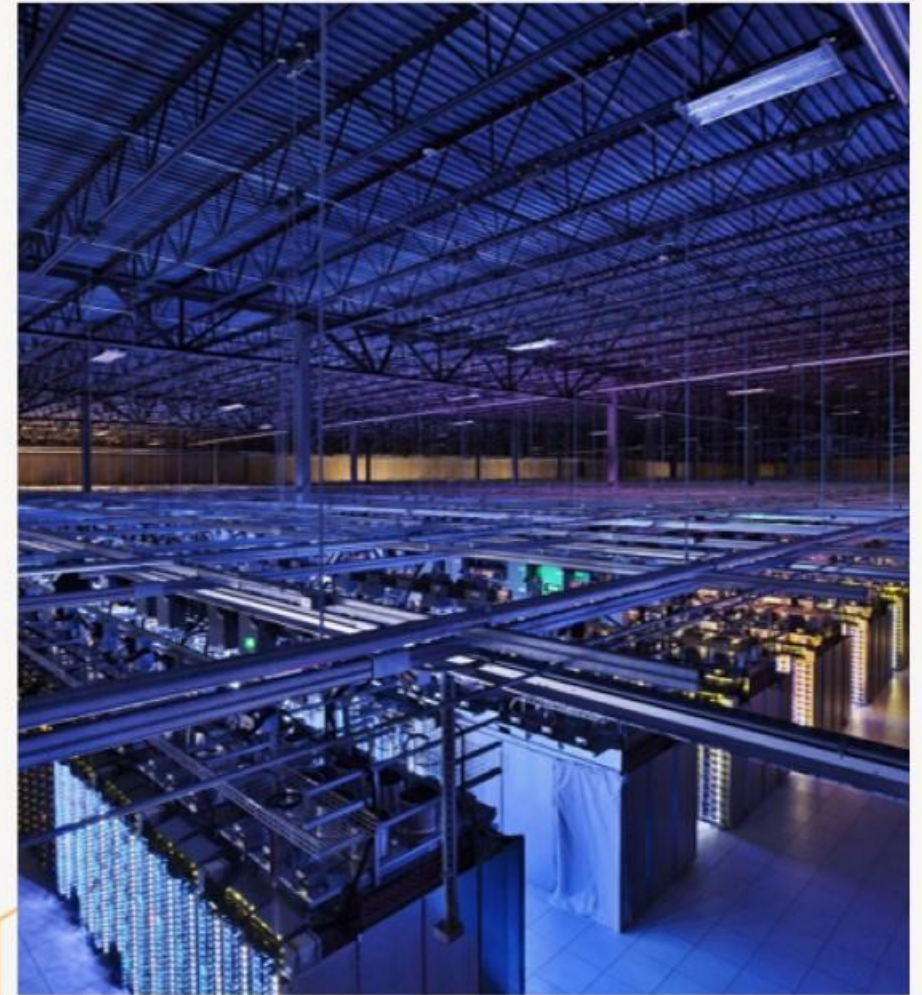
Das BSI hat den Leitfaden im Jahr 2020 als Cloud Computing Compliance Criteria Catalog (C5:2020) überarbeitet. Der C5 ist ein geprüfter Standard, der verbindliche Mindestanforderungen für die Cloudsicherheit und die Einführung von Public Cloud-Lösungen für deutsche Regierungsbehörden und Organisationen, die mit der Regierung zusammenarbeiten, festlegt. Der C5 wird auch zunehmend im privaten Sektor genutzt.

C5 basiert auf international anerkannten IT-Sicherheitsstandards wie

- ISO/IEC 27001:2013,
- Cloud Security Alliance Cloud Controls Matrix 3.0.1 und den
- BSI-eigenen IT-Grundschutzkatalogen.

Der Katalog besteht aus 114 Anforderungen in 17 Bereichen – z. B. der Organisation von Informationssicherheit und physischer Sicherheit – mit Sicherheitsanforderungen, die für alle Clouddienstanbieter gelten, und andere Anforderungen für die Verarbeitung streng vertraulicher Daten und für Situationen, die hohe Verfügbarkeit erfordern.

Quelle: [Cloud Computing-Konformitätskriterienkatalog \(C5\) - Microsoft Compliance | Microsoft Learn](#)



DSGVO

M365

- Im **September 2020** kam die DSK zu dem Schluss, dass ein datenschutzkonformer Einsatz von Microsoft Office 365 auf Basis der damaligen Unterlagen nicht möglich sei.
- Daraufhin gründete die **DSK eine Arbeitsgruppe, die mit Microsoft** in Dialog treten sollte, um datenschutzrechtliche Nachbesserungen zu erreichen.
- In den **nachfolgenden Jahren hat Microsoft wiederholt Änderungen** am Data Protection Addendum (DPA) also der Auftragsdaten Verarbeitung vorgenommen.
- Am **15.09.2022** gab es **erneut** eine DSK wo der Datenschutznachtrag der AVV Auftragsdaten Verarbeitung von Microsoft **kritisiert** wurde
- **Seit** dem von der DSK kritisierten Datenschutznachtrag vom **15.09.2022** hat Microsoft **3 weitere Versionen veröffentlicht**
- die Version vom **01.01.2023**, welche den offiziellen Start der EU Data Boundary, einer europäischen Lösung für die Microsoft Cloud, beinhaltet.
- Die deutschen Datenschutzaufsichtsbehörden haben angesichts der Einführung der EU Data Boundary kurz danach auf der **Zwischenkonferenz 31.01.2023** (S.6) beschlossen, die DPA **01.01.2023** zu prüfen.

Auf der Zwischenkonferenz der DSK am **27.09.2023** führt das **BavLDA** aus (S.4), dass diese Überprüfung erfolgt sei und man nicht davon ausgehe, dass die vorgenommenen Änderungen an dem DSK-Ergebnis der Bewertung der Vereinbarung zur Auftragsverarbeitung für Microsoft 365 von 2022 grundlegend etwas ändern würden.

Eine offizielle, abschließende Bewertung der DPA vom **01.01.2023** durch die deutschen **Datenschutzaufsichtsbehörden** steht jedoch weiterhin **aus**.

Es ist zudem **unklar, ob oder inwiefern die beiden neueren DPA-Versionen schon überprüft worden sind**.

Weitere wesentliche Änderungen in den nachfolgenden DPAs:

- Fassung vom **15.11.2023**: Betonung der Zertifizierung Microsofts nach dem EU-US Privacy Framework, was die Datenübermittlung in die USA auf den neuen Angemessenheitsbeschluss der Europäischen Kommission stützt.
- Fassung vom **02.07.2023**: Erweiterung der EU Data Boundary, wodurch nun alle „personenbezogenen Daten“ und nicht nur Kundendaten darunter fallen.



ADN



ADN

**BREAKING
NEWS**

Wie geht es weiter?

Bundesdatenschutz Beauftragter

Am 20.03.2024 hat der deutsche Bundesdatenschutz Beauftragte im Tätigkeitsbericht gesagt, dass eine laut seiner Auffassung „regelmäßig“ Datenschutzkonforme Nutzung von M365 nicht möglich sei.

Datenschutzbeauftragter der EU-Kommission

Zeitgleich hat der europäische Datenschutzbeauftragte (Zuständig für den Datenschutz der EU-Kommission und anderer EU-Stellen) die Order bzw. eine Verfügung erlassen, dass die EU-Kommission bis zum 09.12.2024 nachweisen muss , dass M365 rechtkonform eingesetzt ist bzw. werden kann.

Es wurden Details gefordert:

- Internationalen Datentransfer unterbinden
- Transparenz herstellen
- Anderen AV-Vertrag mit Microsoft erstellen.

Vorüberlegungen



Paperwork

- Verfahrensverzeichnis anfertigen
- Dokument an Mitarbeiter (Keine Artikel 9 verwenden)
- Datenschutzfolgenabschätzung
- Mit dem Betriebsrat eine Betriebsvereinbarung abschließen



Standort

- M365 Rechenzentrums Standorte in Europa oder Deutschland wählen



Konfiguration

- Abstellung von nicht genutzten M365 Applikationen
- Administration und Konfiguration Einstellungen in Richtung Datenschutz in M365 Lösungen
- Definition der Rollen und Berechtigungen auch auf Einsicht von Daten



Consulting

- Externe Unterstützung von Beratern



Monitoring

- Regelmäßige Kontrolle der Microsoft AV und Anpassung im Unternehmen



DSGVO & KI Innovation

Microsoft AI

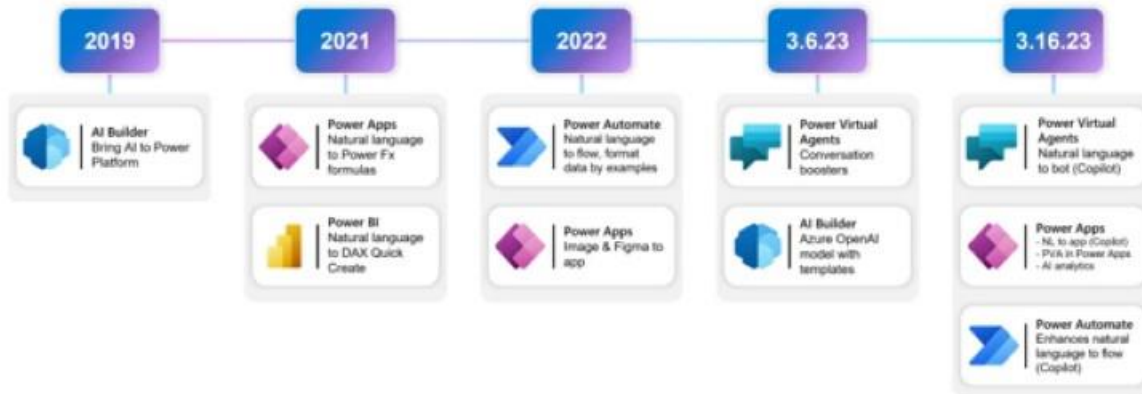
- Power Apps und Power Automate in M365 enthalten (Business und Enterprise Lizenzen)
- Co Pilot nach Datencheck sauber für das Unternehmen einsetzbar
- Zeitersparnis und durch die Analyse von Prozessen und deren Digitalisierung. Mehr Effizienz



Microsoft 365 AI

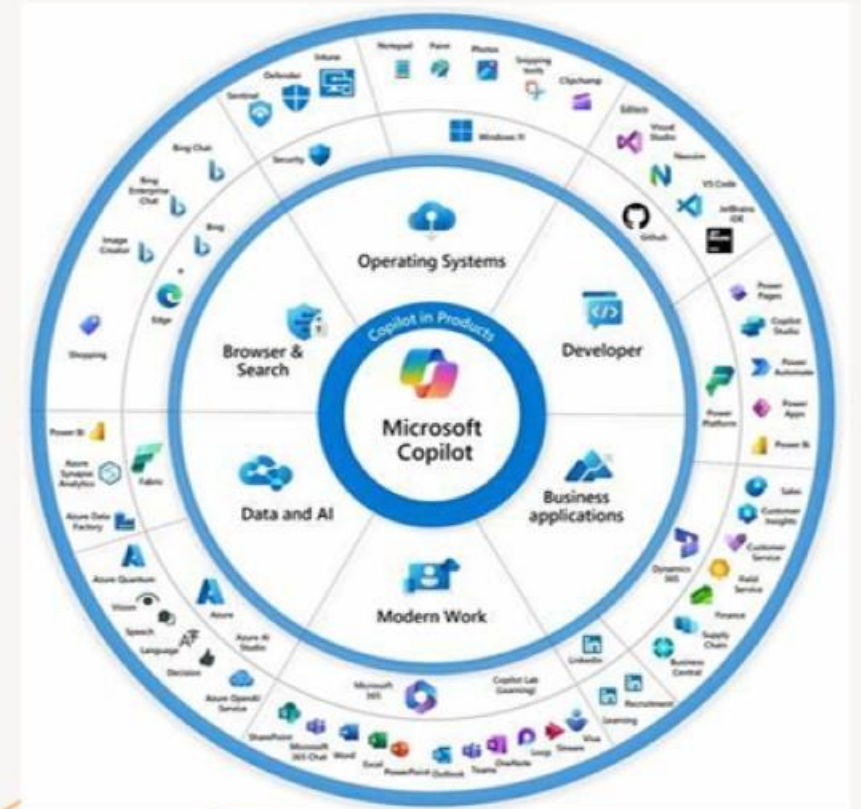
- Power Apps und Power Automate in M365 enthalten
- Integration von den GPT-Modellen sowie AZURE Open AI Modell Templates

Infusing AI in low code since 2019



M365 Co Pilot

- M365 Co Pilot
- Co Pilot Studio
- Co Pilot D365
- Co Pilot Sales & Customer Service
- Co Pilot GitHub



Azure AI

Azure Applied AI Services



Azure Cognitive Search



Azure Form Recognizer



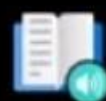
Azure Bot Service



Azure Video Analyzer



Azure Metrics Advisor



Azure Immersive Reader

Azure Cognitive Services



Language



Vision



Speech



Decision



OpenAI







Azure Machine Learning



Azure Machine Learning

DELOS CLOUD

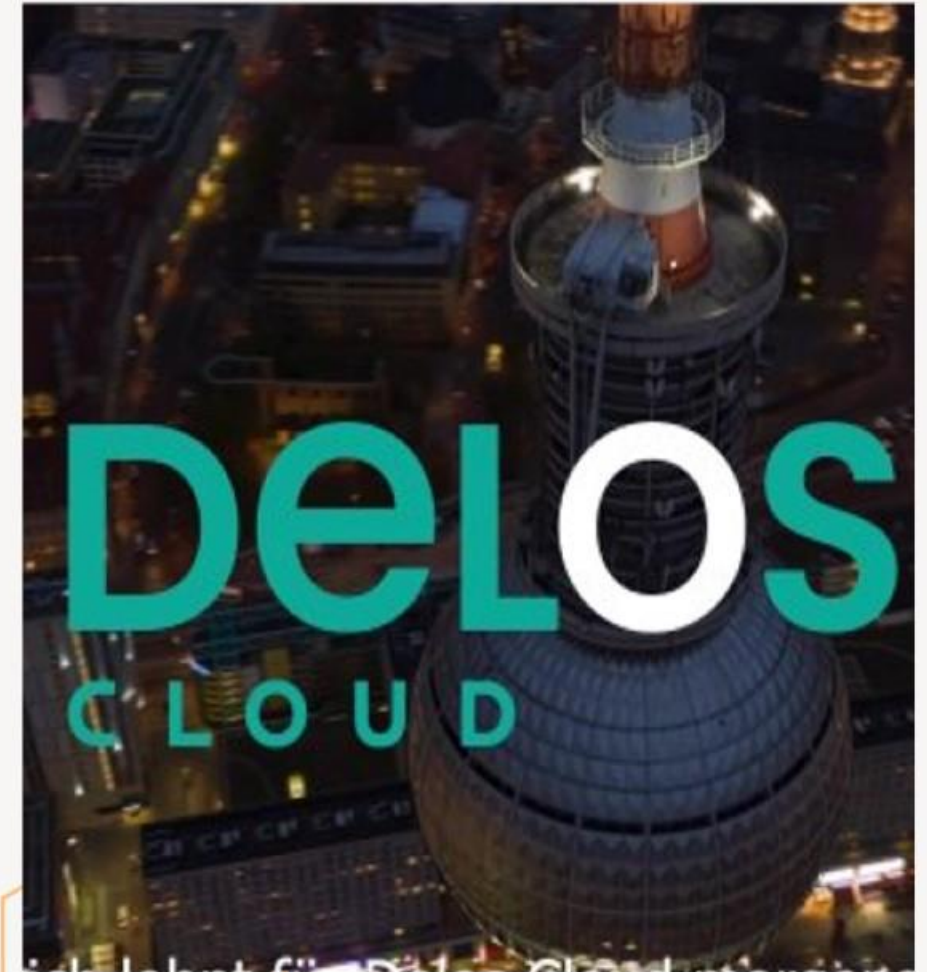
Microsoft und SAP haben eine "souveränen" Cloud entwickelt. Die Rechenzentren werden von Delos als unabhängiges deutsches Unternehmen statt von Microsoft betrieben, sodass US-Behörden rechtlich gesehen nicht auf Daten zugreifen können. Die Cloud ist auch technisch von Microsofts globaler Cloud-Infrastruktur getrennt.

	Grundlegende Schutzbedarfe		Erweiterte Schutzbedarfe
Cloud-Angebot	 Microsoft Cloud	 Microsoft Cloud mit Datengrenze	 DELOS mit Microsoft Technologie
Inhaltsdaten			
Telemetrie & Supportdaten			
Betrieb	durch ein europäisches Tochter-Unternehmen von Microsoft		durch SAP / Arvato Systems
Datenschutz	durch Angemessenheitsbeschluss der EU oder durch Datenschutzfolgeabschätzung		technisch kein ungewünschter Datentransfer möglich

Clouds für unterschiedliche Schutzbedarfe



Microsoft-Cross-Tenant Access zur skalierenden Verwaltung unterschiedlicher Mandanten



DELOS CLOUD

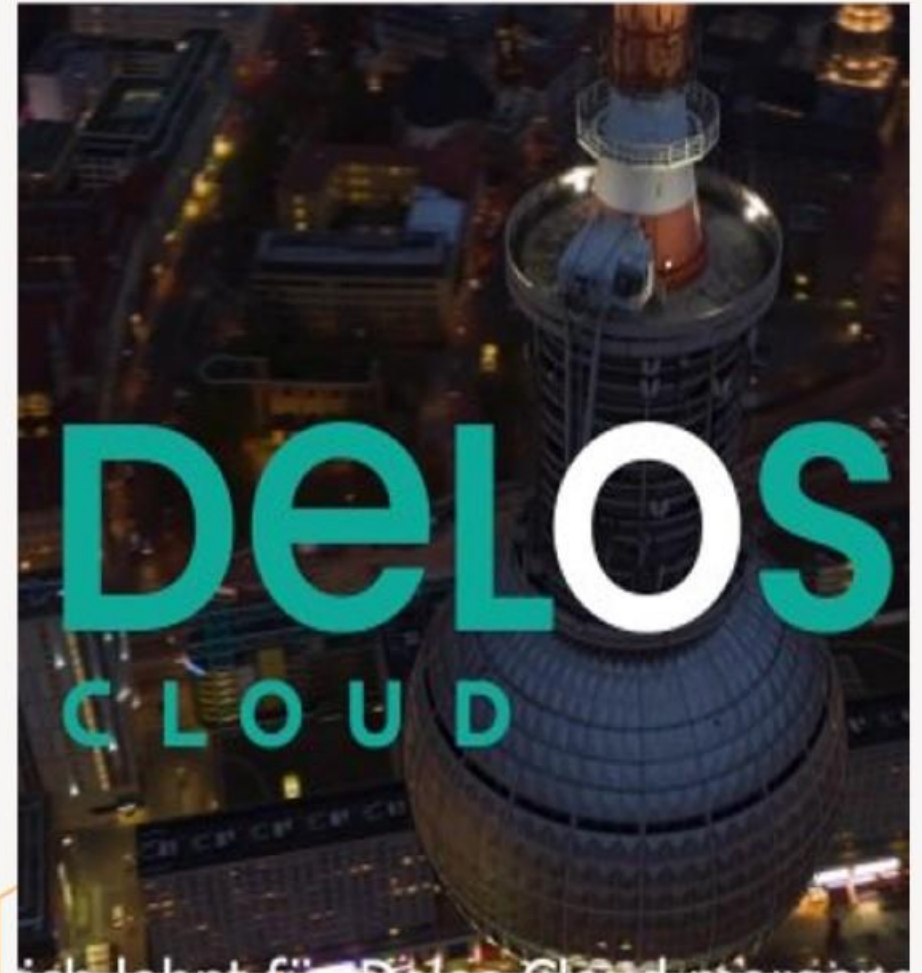
Microsoft und SAP haben eine "souveränen" Cloud entwickelt. Die Rechenzentren werden von Delos als unabhängiges deutsches Unternehmen statt von Microsoft betrieben, sodass US-Behörden rechtlich gesehen nicht auf Daten zugreifen können. Die Cloud ist auch technisch von Microsofts globaler Cloud-Infrastruktur getrennt.



Microsoft 365 E3



Microsoft Azure
Foundational Services



ABN

Fazit

- Vorbereitung und regelmäßige Konfiguration ist wichtig für generelle DSGVO Konforme Nutzung von M365 und anderen Lösungen.
- Durch die DSGVO Vorbereitung auch Vorbereitung auf die Nutzung von KI (Co-Pilot)
- Ab Ende 2024 / Anfang 2025 endlich finale Klarheit





ADN



Danke

Konstantin Gratschow

Fokus Manager Microsoft

ADN Advanced Digital Network Distribution GmbH