SKW Schwarz

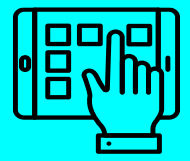
Cloud für Unternehmen

Cloud? Ja, aber (rechts)sicher! – 02. Februar 2023

Dr. Matthias Orthwein, LL.M. (Boston)

Cloud Services – Fluch oder Segen für den Mittelstand?

Cloud Computing ist:



die Bereitstellung von gemeinsam nutzbaren und flexibel skalier-baren IT-Leistungen…

→

durch nicht fest zugeordnete IT-Ressourcen…

→

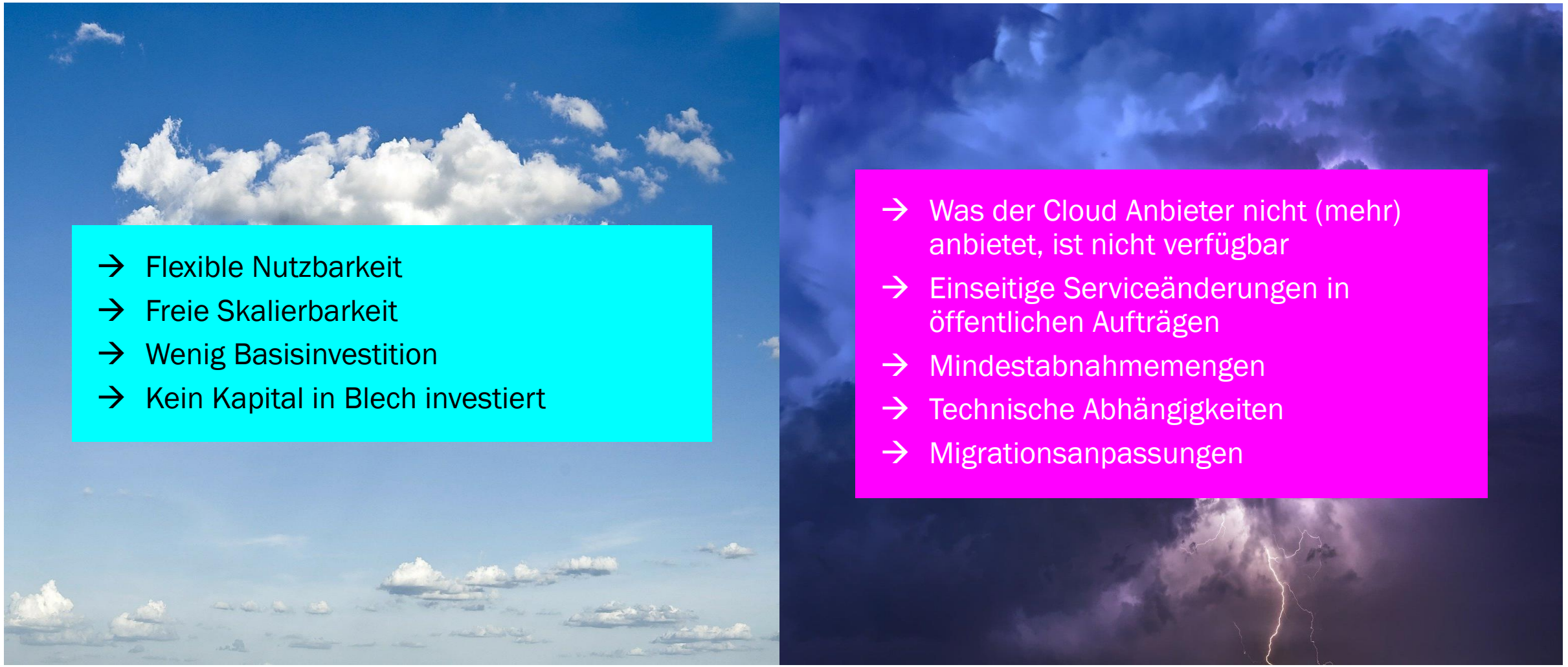
über ein Netzwerk.

Cloud Services – Komfortable Services

- → Unbegrenzt verfügbare Rechenleistung
- → Cloud Ökosystem mit Anwendungsbeispielen
- → Cloud bietet Katalog an fertigen Elementen

- → Hohe Standardisierung
- → SLA sind nicht verhandelbar
- → Datenschutz schränkt Nutzbarkeit in Europa ein?
- → Regulatorische Vorgaben zur Lokalisierung in Europa

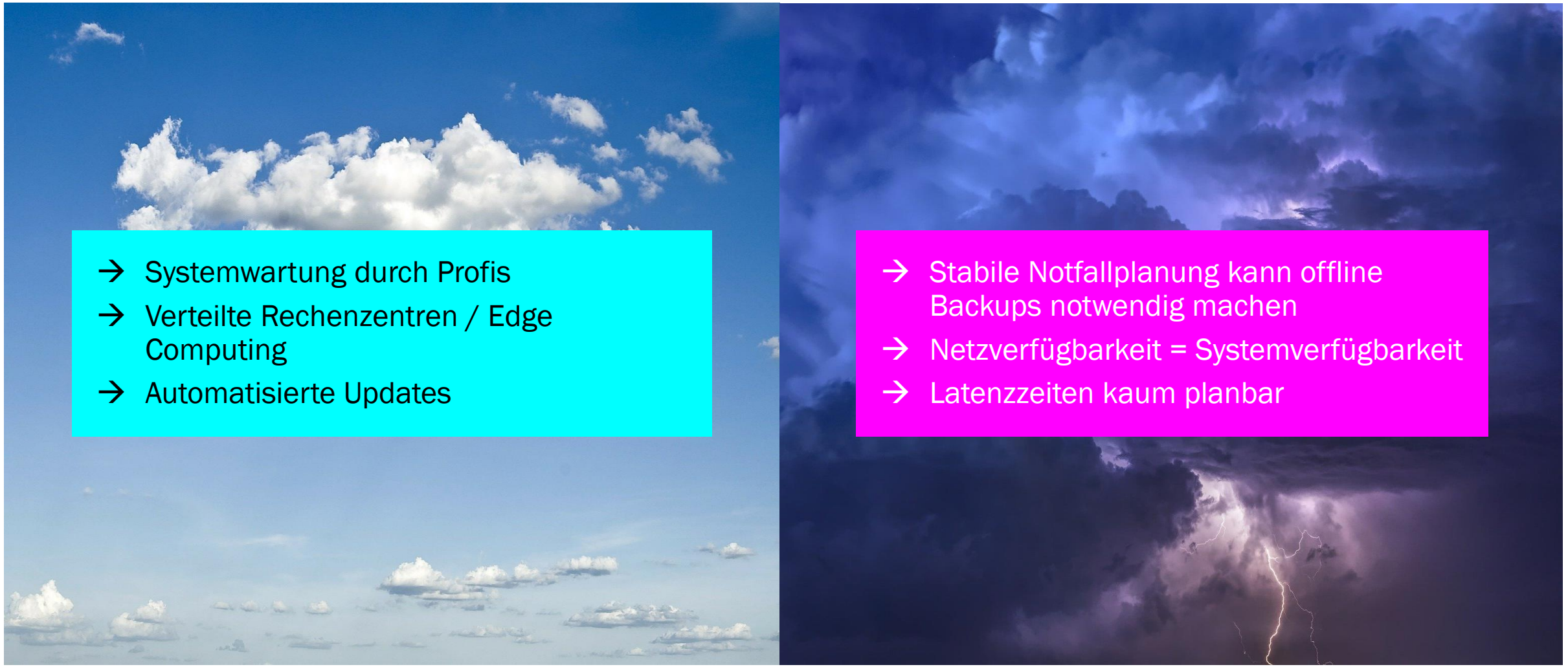
Cloud Services – Flexibilität



- → Flexible Nutzbarkeit
- → Freie Skalierbarkeit
- → Wenig Basisinvestition
- → Kein Kapital in Blech investiert

- → Was der Cloud Anbieter nicht (mehr) anbietet, ist nicht verfügbar
- → Einseitige Serviceänderungen in öffentlichen Aufträgen
- → Mindestabnahmemengen
- → Technische Abhängigkeiten
- → Migrationsanpassungen

Cloud Services – Stabilität



- → Systemwartung durch Profis
- → Verteilte Rechenzentren / Edge Computing
- → Automatisierte Updates

- → Stabile Notfallplanung kann offline Backups notwendig machen
- → Netzverfügbarkeit = Systemverfügbarkeit
- → Latenzzeiten kaum planbar

Cloud Services – IT Sicherheit und Resilienz

- → Hohe Investitionen in IT Sicherheit durch die Betreiber
- → Reduzierte Trefferfläche für individuelle Angriffe
- → Hacker suchen einfache Ziele (z.B. Hafnium)

- → Wer die Cloud hackt, legt alle Nutzer lahm
- → Livesysteme sind keine Archivsysteme
- → Wenig Schutz gegen Sicherheitsbehörden

Cloud Services – Kostenersparnis

- → Freie Skalierbarkeit spart Einmalinvestitionen
- → Standards steigern eigene Effizienz
- → Wettbewerb der Anbieter und freie Wahl zwischen ihnen

- → Preisänderungsrisiko über Laufzeit
- → Hohe Standardisierung
- → Anpassungsbedarf an vorhandene Software
- → Kosten der Migration und Administration
- → Mengendiscounts ohne verbindliche Zusagen

Cloud Services – Strategische Abwägung

Risikoabwägung bestimmt die Cloud Strategie

Cloud Services versprechen:

- Mehr Flexibilität
- Geringere Kosten
- Mehr Stabilität
- Bessere Resilienz
- Komfortable Services

Risiken in der Cloud:

- Vertragliche Risiken
- Datenschutz-risiken
- Regulatorische Risiken

Compliancepflicht der Geschäftsführung:

- Geschäftsführung/Vorstand haften persönlich, dass Unternehmen so organisiert sind, dass **Gesetze nicht verletzt** werden und alle **Risiken für den ordnungsgemäßen Geschäftsverlauf** rechtzeitig erkannt und mit den Chancen im Einklang stehen;
- Diese Organisation muss **überwacht** und regelmäßig **überprüft** werden, § 93 Abs. 2 AktG, § 43 Abs. 2 GmbHG

→ **Cloudstrategie bedeutet daher Risikoanalyse und Bewertung**

Cloud Services – Individuelle Analyse

Vorüberlegungen durch Klassifizierung von Cloud Risiken

Bevor Daten/Applikationen in die Cloud gelegt werden, empfiehlt sich die Klassifizierung, ob diese Daten/Applikationen überhaupt für den Einsatz in der Cloud in Frage kommen:

- → Schutzbedarf anhand **Sicherheitseinstufung**
  („geheim“/Schutzklasse 3 meist nicht Cloud fähig;
  Schutzklasse 2 nur verschlüsselt)
- → **Datenschutz**:
  personenbezogene Daten dürfen nur in sichere Drittstaaten, nur mit zusätzlichem Schutz in unsichere Drittstaaten oder sind zu anonymisieren
- → **Verfügbarkeitseinstufung**:
  Wie wichtig ist der unterbrechungsfreie Zugriff und welcher Schaden droht bei Ausfall?
- → **Lokalisierungs-** oder Systemvorgaben (DATEV) von Kundenseite beachten
- → Risiko des Zugriffs durch **Dritte** (Behörden, Hacker, Admins)
- → Bewertung der **Sicherheitsmaßnahmen** (Verschlüsselung, Zertifikate etc.)

Compliance, Datenschutz & Cloud

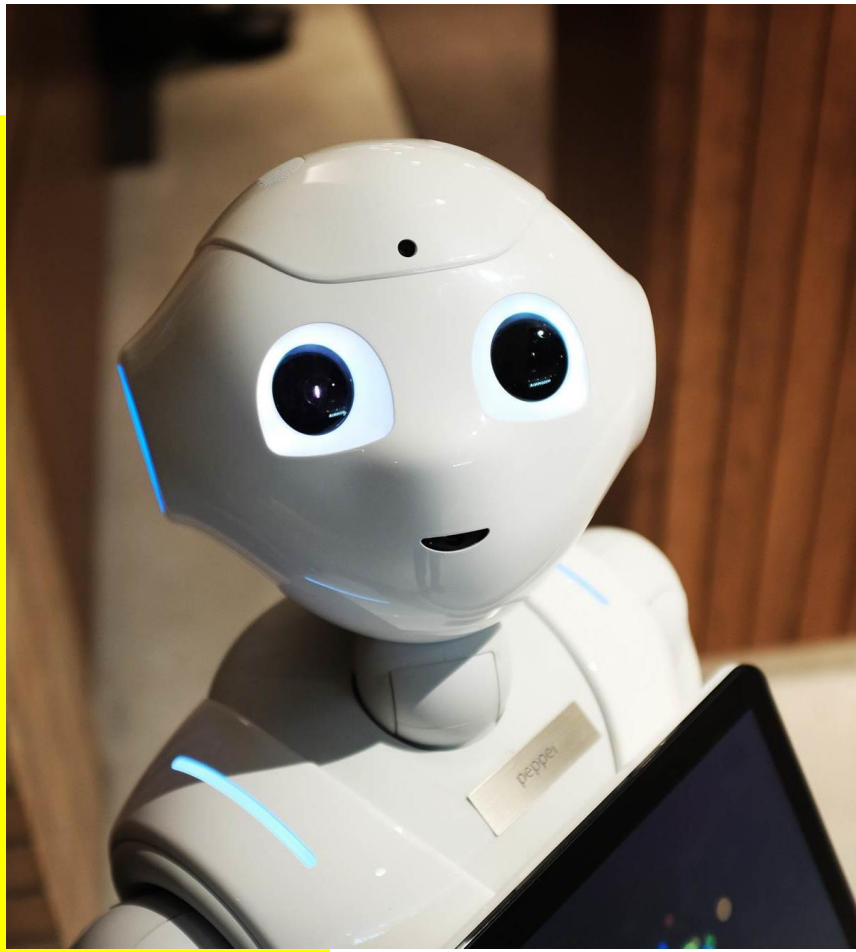
Das Problem

- → **DSGVO** verlangt **Garantien für den Schutz personenbezogener Daten** beim Transfer aus der EU oder Zugriff von außerhalb der EU, die das US Recht insbesondere den nicht-US Bürgern nicht gibt
- → US Cloud Anbieter können diese Garantien auch nicht allein durch Vertragsversprechen herstellen, weil das **US Recht zwingend** und nicht abwendbar ist
- → Der EuGH hat auf Klagen von **Max Schrems** schon zweimal Versuche von EU und USA für unzureichend erklärt, die Situation durch staatliche Abkommen zu regeln
- → Technisch ist in der Cloud auch bei **Server Standort („Tenant Location“) „Europe“** nicht auszuschließen, dass Support aus den USA zugreifen muss oder dass Informationen über aktuelle Sicherheitsbedrohungen global über alle Tenants ausgetauscht werden
- → Zusatzrisiko: Telemetriedaten, die Cloud Provider für eigene Zwecke nutzen

Compliance, Datenschutz & Cloud

Die Anforderungen

- → Wer für die Erhebung und Verwendung der Daten verantwortlich ist, muss Rechenschaft darüber ablegen, wie, für welchen Zwecke, wo und auf welcher Rechtsgrundlage er Daten verarbeitet (**Rechenschaftspflicht**, Art. 5 DSGVO)
- → Wenn Daten die EU verlassen oder von außerhalb der EU darauf zugegriffen wird, muss der Verantwortliche die damit verbundenen Risiken beurteilen (**Transfer Impact Assessment**, TIA)
- → Dienstleister dürfen nur eingesetzt werden, wenn deren Datenschutzniveau geprüft und ein Auftragsverarbeitungsvertrag abgeschlossen ist (**AVV**)
- → Wenn der EU Mustervertrag zum Datentransfer (**SCC**) z.B. wegen zwingender Gesetze nicht alleine ausreicht, um Daten zu schützen, müssen zusätzliche Sicherheitsgarantien geschaffen werden: **vertraglich**, **technisch** und **organisatorisch**



Compliance, Datenschutz & Cloud

Der (rechtliche) Stand der (Microsoft) Dinge

- → Die Musterklauseln der EU (SCC) dürfen seit Ende 2022 nur noch in der Version von Juni 2021 verwendet werden: **ggf. aktualisieren**
- → Sobald die EU Kommission die **Executive Order von Präs. Biden** vom 7.10.2022 als gleichwertigen Datenschutz anerkennt, genügt AVV ohne SCC
- → Microsofts Datenschutzergänzung zum Lizenzvertrag (DPA) reicht nach Meinung der **Deutschen Datenschutzbehörden** alleine nicht aus (25.11.2022)
- → Microsoft hat zum **1.1.2023 neue Version des DPA** zu allen Lizenzformen veröffentlicht: sagt ausdrücklich Unterstützung der Rechenschaftspflicht des Kunden zu, muss für Altlizenzen gesondert vereinbart werden
- → Zusätzliche technische Garantien: **EU Data Boundaries, Hold your own key, Ausschalten von Telemetriefunktionen**
- → Zusätzliche organisatorische Garantien: **MS Purview** und **Customer LockBox**
- → Kunde muss mit **TIA dokumentieren**, dass Datenflüsse klar erkennbar und ausreichend abgesichert sind

Dr. Matthias Orthwein, LL.M. (Boston)

Rechtsanwalt / Partner

→ Follow me on **LinkedIn**: www.linkedin.com/in/dr-matthias-orthwein-ll-m-boston-7989952

→ Oder auf unserer **Webseite**: www.skwschwarz.de/personen/matthias-orthwein

+49 89 28640-102

m.orthwein@skwschwarz.de

Wittelsbacherplatz 1

80333 München


SKW
Schwarz