TeleTrusT Information Security Professional

TeleTrusT Professional for Secure Software Engineering

TeleTrusT Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

T.I.S.P./T.P.S.S.E. Community Meeting 2024

Berlin, 05. – 06.11.2024

Microsoft 365

Datenschutz & rechtskonformer Einsatz

Kristin Benedikt, Thomas Floß
EDV-Unternehmensberatung Floß GmbH

Quelle des Logos: https://commons.wikimedia.org/wiki/File:Microsoft_365.svg#/media/File:Microsoft_365.svg

Ihre Referentin

Kristin Benedikt

- Richterin am Verwaltungsgericht
- Behördliche Datenschutzbeauftragte
- Wirtschaftsmediatorin
- Referentin und Autorin zum Datenschutz, ePrivacy-Recht und zur Künstlichen Intelligenz

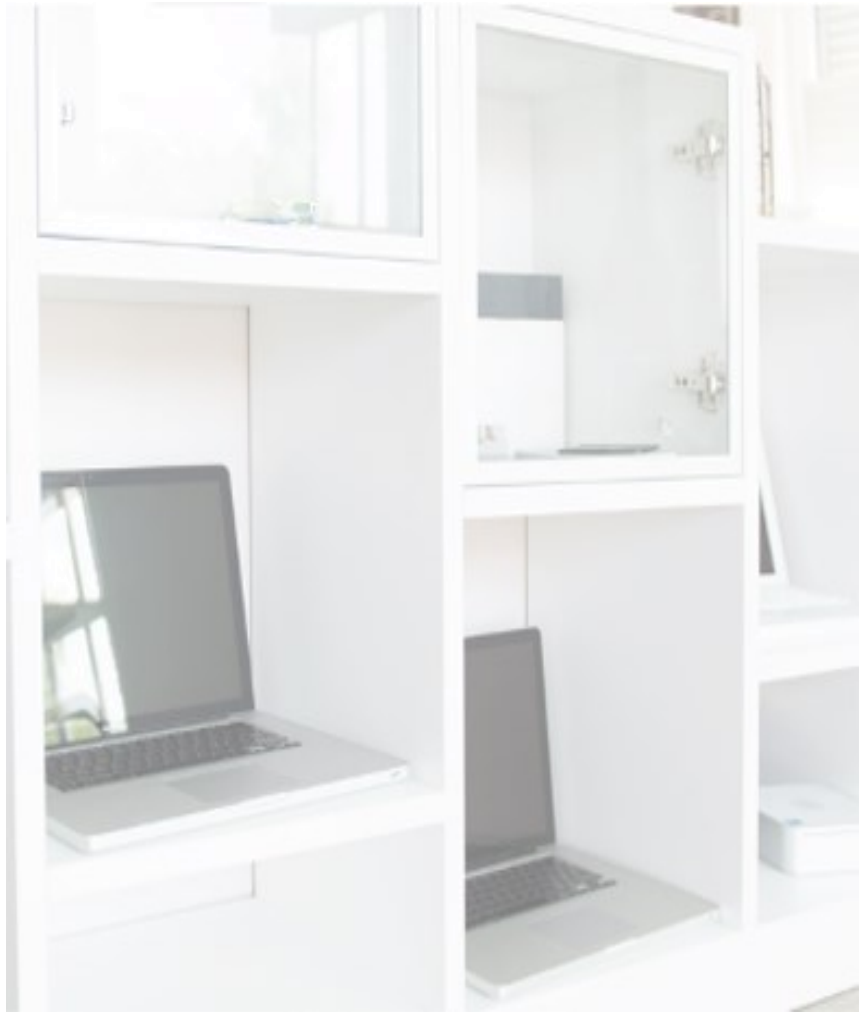
Ihr Referent

Thomas Floß

- geprüfter Datenschutzbeauftragter (TÜV / udis)
- Teletrust Information Security Professional (T.I.S.P.)
- geprüfter EDV-Sachverständiger
- Certified Ethical Hacker (CEH)
- IT-Forensiker
- geprüfter IT-Compliance Officer (TÜV)
- Certified Information Systems Auditor (CISA)
- Certified Data Privacy Solutions Engineer (CDPSE)

Agenda

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



- Der Weg in die Cloud
- Microsoft 365, was ist das?
- Rechtsgrundlagen und Besonderheiten
- Telemetriedaten
- Datentransfer in die USA / Drittstaaten
- Technische + organisatorische Maßnahmen
- MS Copilot

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Der Weg in die Cloud

Microsoft 365, Google Cloud, AWS & Co

Der Weg in die Cloud

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Warum in die Cloud, das ist doch nicht sicher, oder?
Schauen wir mal auf die Fakten:

- Tagtäglich erfolgenden tausende von Hackerangriffen auf unsere Infrastrukturen
- Die Administratoren müssen täglich dutzende wenn nicht hunderte von Systemen patchen
- Wöchentlich gibt es neue Zero-Day Exploits
- Es gibt einen enormen Fachkräftemangel von **wirklichen** Sicherheitsexperten
- Hacking ist ein lukratives Geschäft geworden

Der Weg in die Cloud

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Ist die Cloud denn besser?

- Bei der „richtigen“ Auswahl des Anbieters: **JA**
- Cloudanbieter wie Microsoft, Google, Amazon, Apple & Co. haben extrem sichere Infrastrukturen und sehr gut ausgebildetes und spezialisiertes Fachpersonal
- „Gute“ Cloudanbieter haben 24*7*365 Sicherheitssupport mit professionellen SOC‘s (Security Operation Centern)

- ABER, bzgl. des Datenschutzes ist es schon eine Herausforderung

Der Weg in die Cloud

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Denn die großen Anbieter sind meistens US-Firmen und diese unterliegen dem CLOUD sowie FISA-Act.

Hier liegt die Herausforderung in Bezug auf die unterschiedlichen Rechtsnormen, **aber** dies ist durch gezieltes und richtiges Vorgehen „heilbar“.

Der Weg in die Cloud

Stichworte sind dabei u.a.:

- Verschlüsselung
- Klassifizierung
- Risikoanalyse
- richtige Konfiguration
- klare Richtlinien und Vorgaben
- …

Der Weg in die Cloud

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Fazit:

In der heutigen Zeit sind die Daten & Informationen aus
der technischen Sicht in einem professionellen Rechenzentrum
mindesten 100 x besser aufgehoben als im Serverraum,
der sich im Keller befindet.

Nutze ich dann noch „professional Services“ drum herum,
wie z.B. eine Microsoft 365 (MS 365) Welt,
dann senke ich das (technische) Risiko immens!

Microsoft 365, was ist das denn genau?

Microsoft 365, was ist das?

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Es gibt innerhalb des Microsoft Kosmos dutzende Pakete, von:
  - Home & Family
  - Business Pakete (für KMU‘s)
  - Enterprise Pakte
  - Teamspakete
  - ….

Quelle: Wikipedia

Microsoft 365, was ist das?

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- **Folgende Lizenz-Pakte stehen zur Verfügung (Stand Mitte 2024)**

Microsoft 365 Licensing

By Aaron Dinnage — **July, 2023**

Enterprise Mobility + Security (EMS)	All	Simple	E3	E5	Intune	
Microsoft Entra*	Entra ID (All)	Entra ID (Paid)	ID Governance	Workload ID		
Microsoft 365 Apps	All	Business	Enterprise			
Microsoft 365 Business	All	Basic	Standard	Premium		
Microsoft 365 Consumer	All	Family	Office			
Microsoft 365 Education	All	A1 (Legacy)	A1 for Devices	A3	A5	
Microsoft 365 Student Use Benefit	All	Simple				
Microsoft 365 Enterprise	All	Venn	Landscape	E3	E5	
Microsoft 365 Frontline	All	F1	F3	F5		
Microsoft Defender	Business	Endpoint	Office 365	Servers	CSPM	Vuln Mgmt
Microsoft Project and Visio	Project	Visio				
Microsoft Teams	Premium	Rooms	Rooms Basic	Rooms Pro		
Office 365 Education	All	Simple				
Office 365 Enterprise	All	Simple	E1	E3	E5	F3
Windows	Enterprise	Pro	VL	Windows 365	W365 Compare	
Client Access License (CAL)	CALs	Main Bridges	Other Bridges	All Bridges		

Quelle: https://m365maps.com/

Microsoft 365, was ist das?

- **Wie steht es mit der Sicherheit?**

  - Einer neuer Tenant hat standardmäßig wenig/nicht alle erforderlichen Sicherheits- wie Datenschutzeinstellungen

  - In den kleinen Paketen gibt es wenige / keine Sicherheitstools (Defender, Intune, etc.)
    - Microsoft lässt sich Sicherheit bezahlen

Microsoft 365, was ist das?

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Fazit:

Einer neuer Tenant hat standardmäßig nur eine mittlere Sicherheit.

Die „kleinen“ Pakte beinhalten keine „wirkliche“ Verschlüsslung.

Beim großen Paket (E5) gibt es Verschlüsselungstechniken

Wird die Microsoft Verschlüsselung genutzt, so funktionieren die meisten Dienste uneingeschränkt.

Rechtsgrundlagen und Besonderheiten für den Einsatz

Rechtsgrundlagen und Besonderheiten für den Einsatz

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Keine spezifische Rechtsgrundlage für den Einsatz nötig, da MS 365 nur ein Mittel zur Verarbeitung ist

- Rechtsgrundlage ergibt sich aus Zweck der Datenverarbeitung
  - Beschäftigtendaten
  - Kundendaten
  - Kommunikation
  - Marketing etc.

Rechtsgrundlagen und Besonderheiten für den Einsatz

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Erforderlichkeitsgrundsatz wird über TOMs Rechnung getragen

- Grundsätzlich keine DSFA nötig, da Einsatz von MS 365 nicht per se zu einem hohen Risiko der Datenverarbeitung führt

Rechtsgrundlagen und Besonderheiten für den Einsatz

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Eigene und Microsofts Verarbeitungszwecke müssen bei rechtlicher Bewertung getrennt beurteilt werden

- Bei Telemetriedaten und Diensten zur elektronischen Kommunikation sind zusätzlich die Regelungen des TDDDG zu beachten
  - § 25 TDDDG regelt den Schutz der Geräteintegrität
    - Keine datenschutzrechtliche Regelung!
    - Gilt auch bei juristischen Personen und anonymen Daten
  - Zugriff/Speicherung erfolgt grundsätzlich durch Microsoft

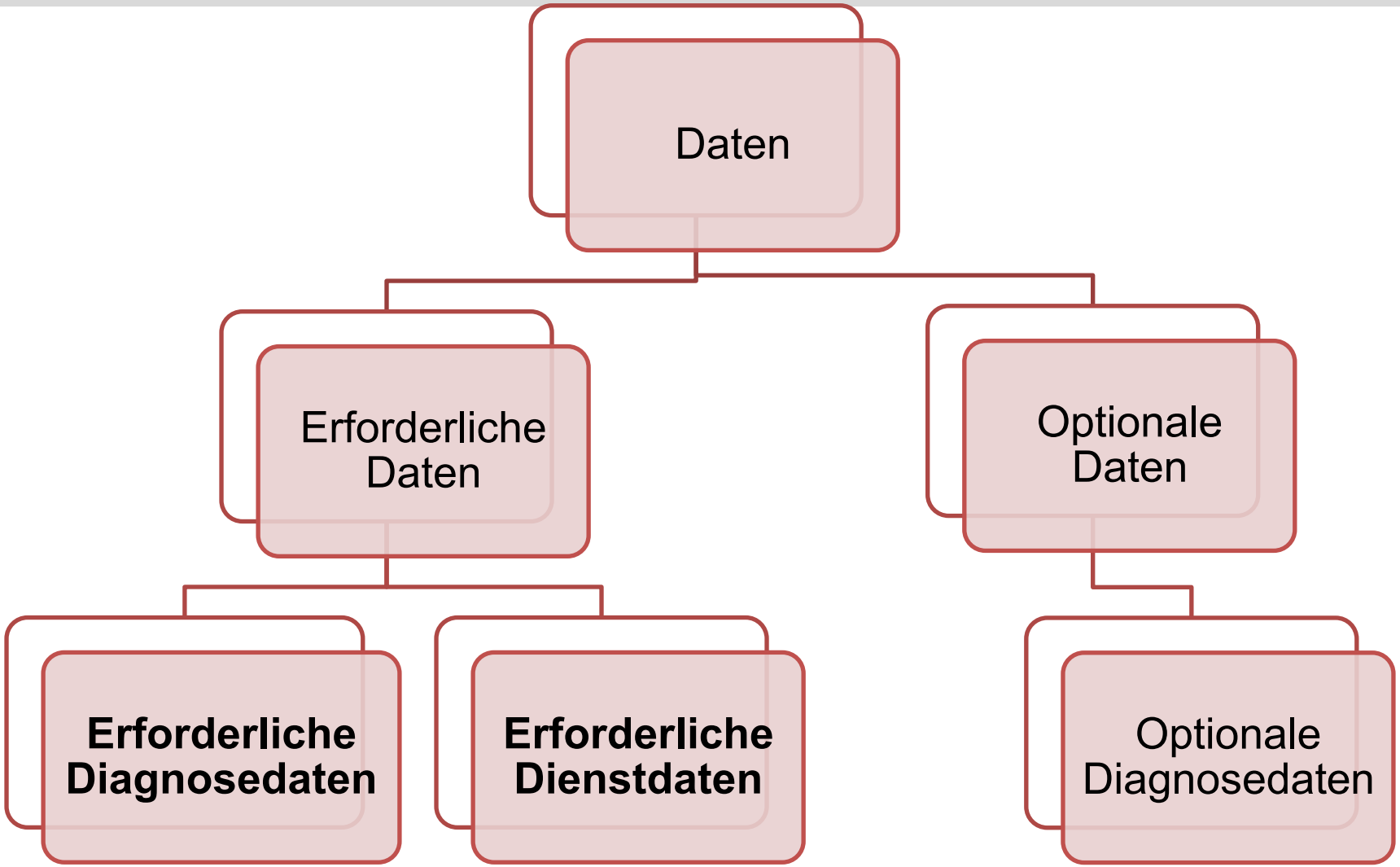
Rechtsgrundlagen und Besonderheiten für den Einsatz

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Telemetriedaten dienen primär der Fehleranalyse
- Wichtig, die „Tiefe“ der Telemetrieinformationen ist einstellbar
- Alle Betriebssysteme wie auch sehr viele Anwendungen senden Telemetrieinformationen

Telemetriedaten

Telemetriedaten bei Microsoft



Telemetriedaten bei Microsoft

Datenkategorie	Beschreibung	Beispiele
Gerätekonnektivität und -konfiguration	umfasst Details zum Gerät, zur Konfiguration und zu den Verbindungsfunktionen	Diagnoseinformationen zur Internetverbindung des Benutzers, um zu verstehen, wie sich dies auf die Konnektivität mit Office-Diensten auswirken kann.
Leistung von Produkten und Diensten	umfasst Details zur Integrität und Leistung des Geräts oder Dienstes	Das Ereignis, das normale und fehlerhafte App-Beendigungen zur weiteren Untersuchung erfasst.
Nutzung von Produkten und Diensten	umfasst Informationen zur Installation und Aktualisierung von Software auf dem Gerät	Ereignisse, die generiert wurden, um festzustellen, ob eine Datei erfolgreich geöffnet oder gespeichert wurde.
Softwareinstallation und -bestand	umfasst Informationen zur Installation und Aktualisierung von Software auf dem Gerät	Informationen über das Laufzeitverhalten von benutzerdefinierten Add-In-Funktionen in Excel.

Datentransfer in die USA / Drittstaaten

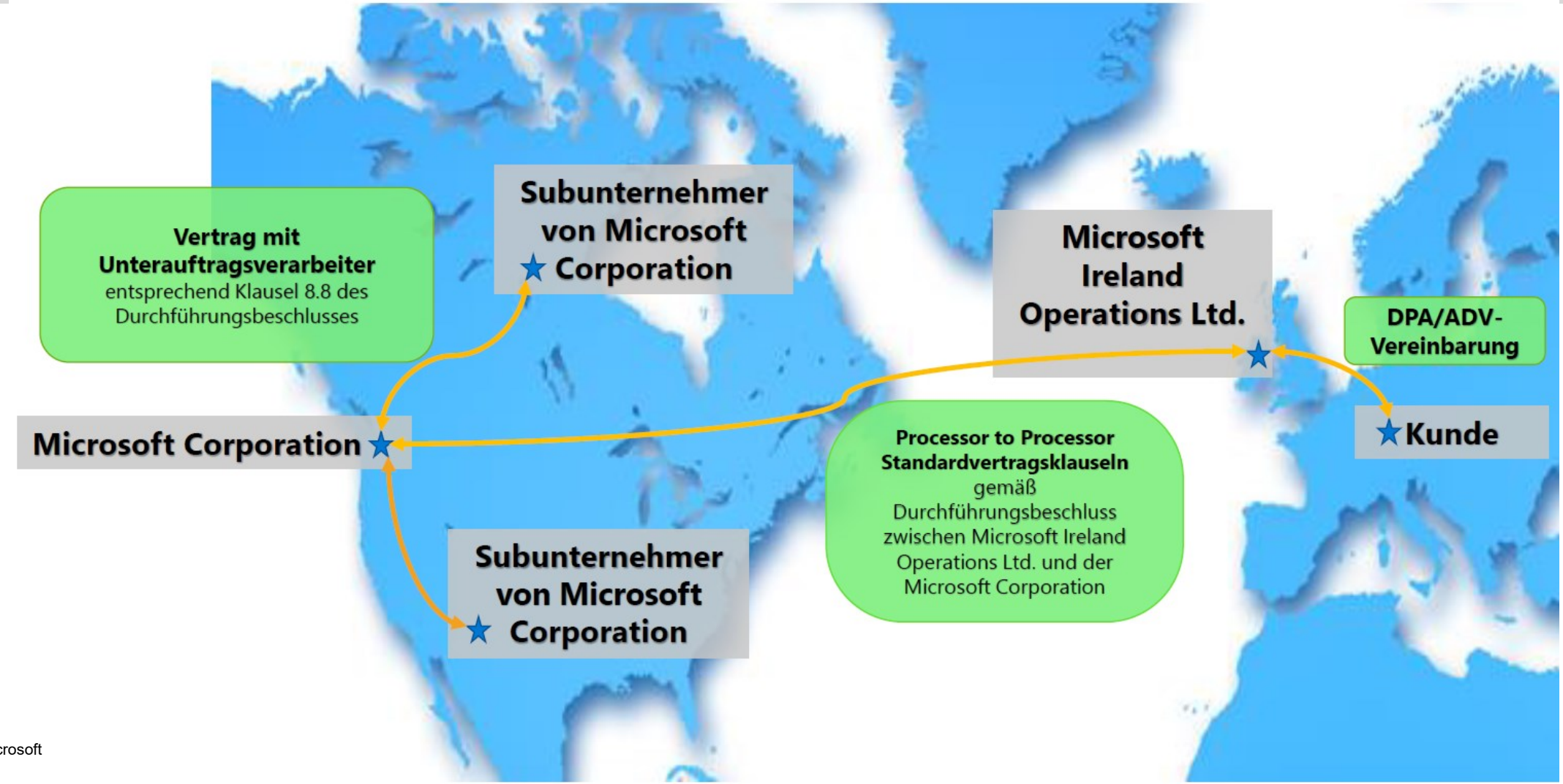
Datentransfer in die USA

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Wichtige Grundsätze des TADPF (Trans-Atlantik Data Privacy Framework):
  - ➢ Zugriff der US-Geheimdienste auf notwendige und verhältnismäßige Maß beschränkt
  - ➢ neues zweistufiges Rechtsbehelfssystem zur Untersuchung und Beilegung von Beschwerden von EU-Bürgern
  - ➢ Verpflichtung zur Selbstzertifizierung durch U.S. Department of Commerce

Datentransfer in die USA

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



Quelle: Microsoft

Datentransfer in die USA

+ Anhang C (Additional Safeguards Addendum)
  - Anfechtung von Anordnungen
  - Entschädigung von betroffenen Personen
  - Zertifizierung
  - Verschlüsselung
  - Ausübung von Rechten
  - Double Key Encryption

Quelle: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Datentransfer in die USA

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

SCC zwischen Microsoft Ireland und Microsoft Corporation	Mit ergänzenden Maßnahmen
AVV zwischen Kunden und Microsoft	Mit ergänzenden Maßnahmen aus SCC
EU Data Boundary	

Datentransfer in die USA

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Microsoft bietet ab Ende 2022 ausschließlich Datenverarbeitung innerhalb der EU an
- Gilt für alle Cloud-Dienste
- EU Data Boundary steht Unternehmen und öffentlichen Stellen zur Verfügung

Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Für eine rechtssichere Verarbeitung innerhalb der Microsoft 365 Cloud sind aus technisch / organisatorischer Sicht die folgenden Schritte fundamental wichtig:

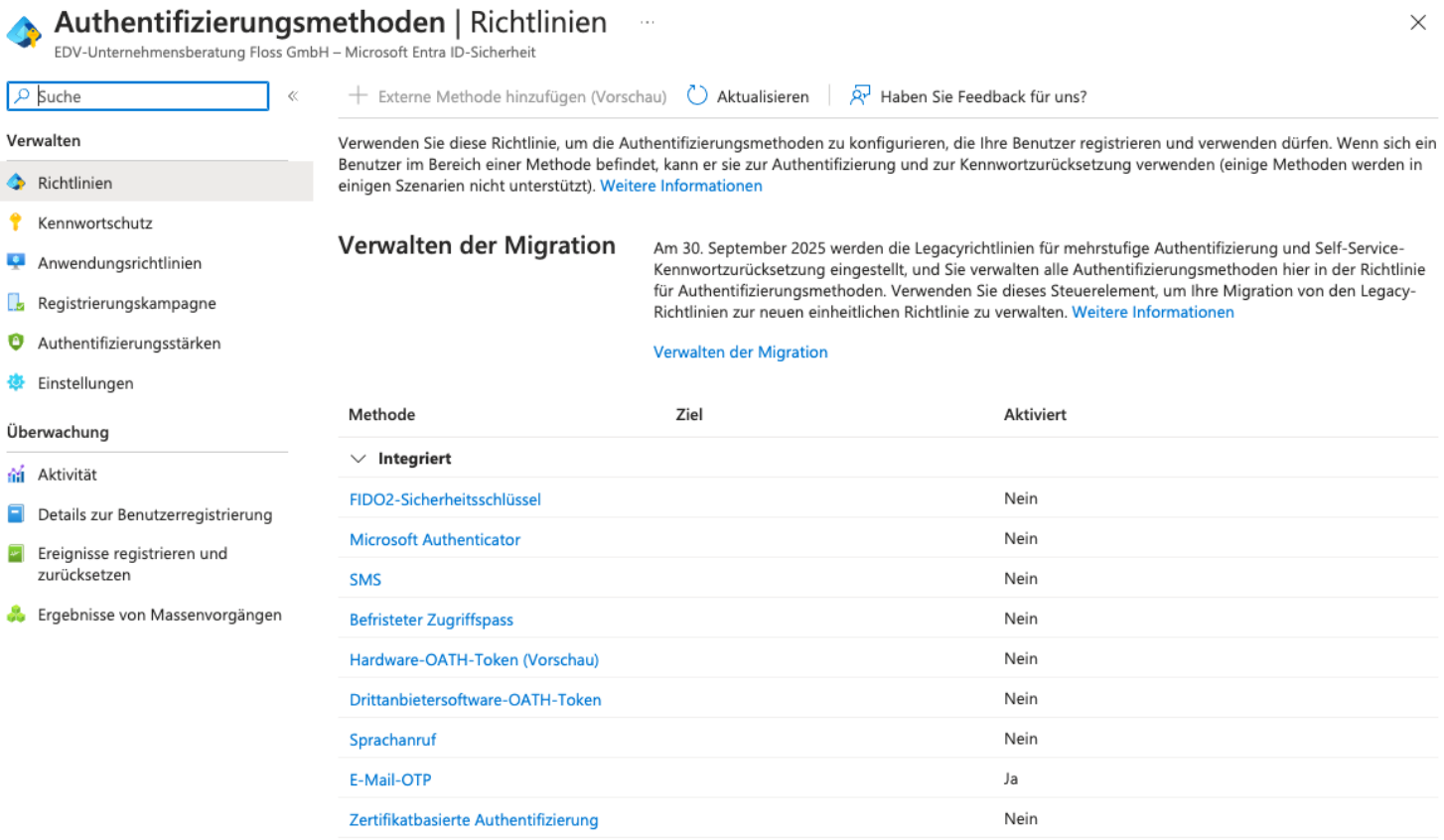
Technische und organisatorische Maßnahmen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

1. Schutzbedarfsanalyse & Risikobetrachtung
2. Datenklassifizierung (öffentlich, intern, vertraulich ...)
3. Technische Maßnahmen wie Berechtigungskonzept, Verschlüsselung
4. Richtlinien (Informationssicherheit, Acceptable Use, …)
5. Datensicherungskonzept

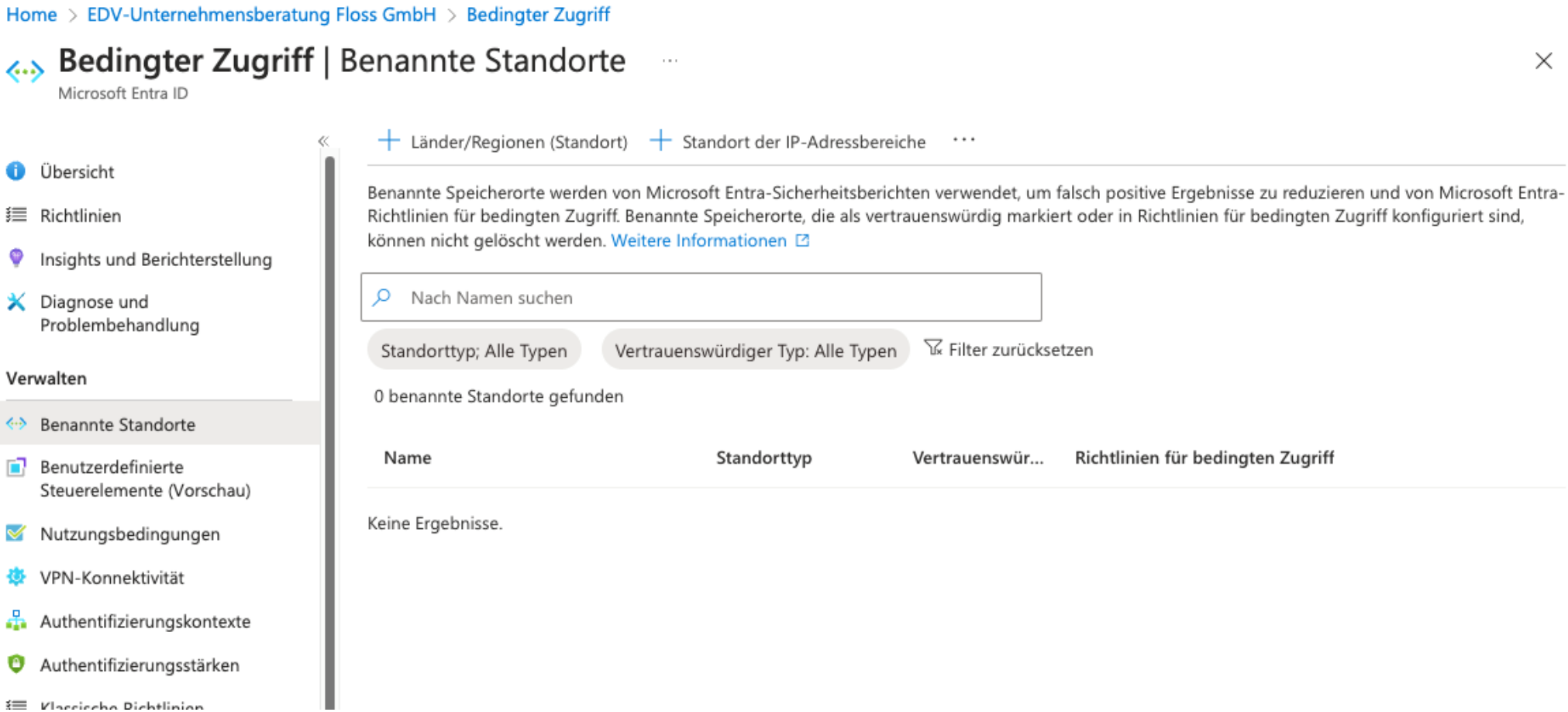
6. Business Continuity (Notfallpläne, Prozessabläufe)
7. Desaster Recovery (je nach Nutzung)
8. Change Prozesse
9. Systemdokumentation
10. Verträge

Die wichtigsten Fakten: 2 Faktor Authentifizierung



Quelle: Microsoft Entra Admin Center □ Schutz □ Authentifizierungsmethoden

Die wichtigsten Fakten: Zugriff begrenzen



Microsoft 365 Entra Admin Center Bedingter Zugriff -> Benannte Standorte

Technische und organisatorische Maßnahmen

Die wichtigsten Fakten: getrennte Adminkonten

- **Kein** normaler User hat Adminrechte!
- Ein Admin benötigt keine zugewiesenen Lizenzen!
- Klar definierte “Named Admin“ Konten sind vorhanden!
- Ggf. Abstufung der Adminfunktionen (Exchange, Sharepoint, etc.)

Die wichtigsten Fakten: Verschlüsselung
Im Microsoft 365 Umfeld gibt es mehrere Verschlüsselungsmechanismen, jedoch nur wenige sinnvolle:

- **Verschlüsselungsoptionen im E5 Paket**

  - Vorteile:
    - (fast) volle Funktionalität der Services, da der Schlüssel zentral bei Microsoft liegt
    - mögliche Angreifer kommen nicht an den Schlüssel heran
    - zentrale Verwaltung bei Microsoft

Die wichtigsten Fakten: Verschlüsselung

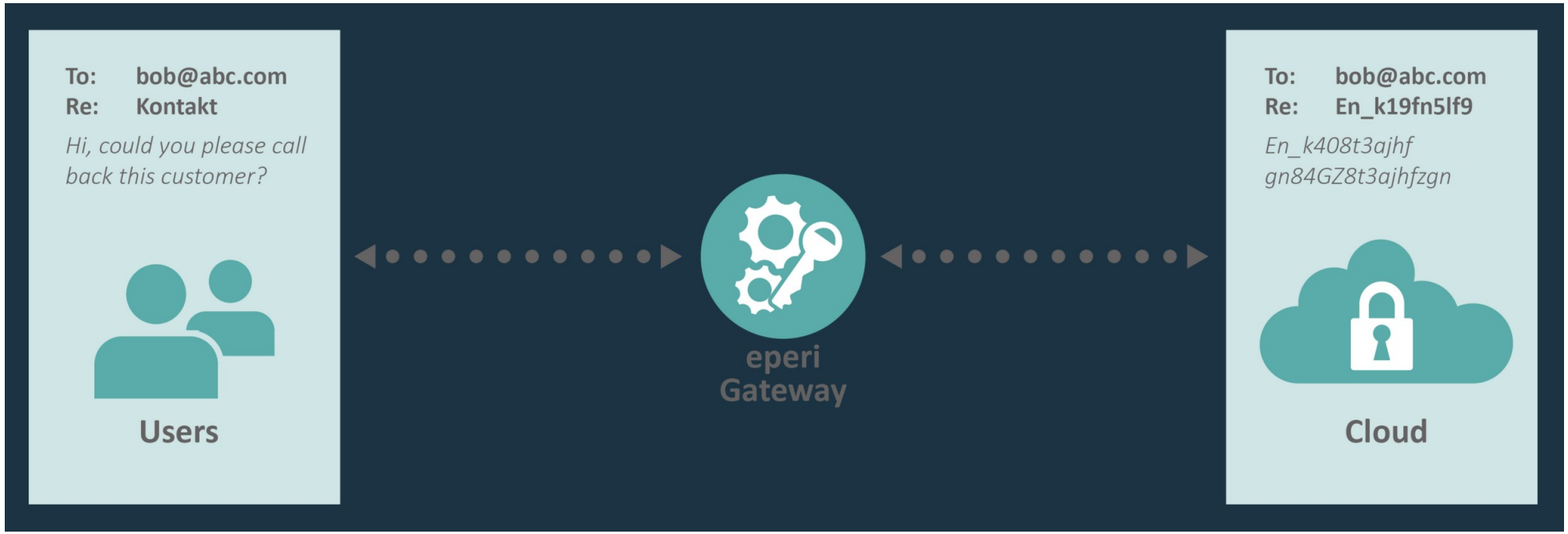
- Nachteile:
  - Der Schlüssel liegt unter der „Fußmatte“, somit keinen wirklichen Schutz in Bezug auf den CLOUD und FISA-Act
  - Die DSK (Datenschutzkonferenz) sieht diese Art von Verschlüsselung als „kritisch“
  - Aus Informationssicherheitssicht ist eine solche Lösung (Schlüssel liegt im Rechenzentrum / beim Anbieter) keine sinnvolle Variante

Technische und organisatorische Maßnahmen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

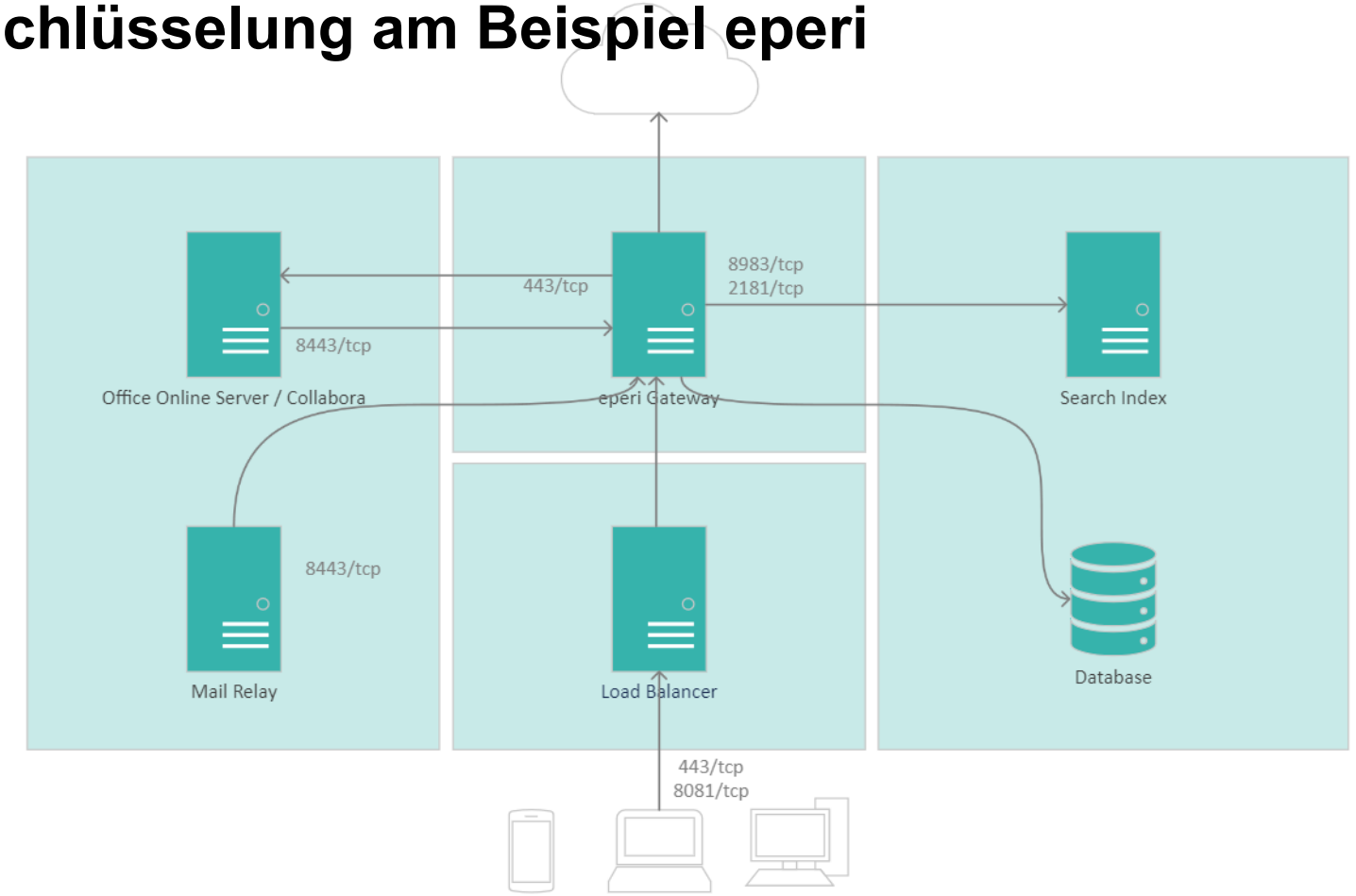
Nun die Lösung der Herausforderungen,
Verschlüsselung außerhalb der Microsoft Welt

„Richtige“ Verschlüsselung am Beispiel eperi



Quelle: Copyright: eperi GmbH (mit freundlicher Genehmigung)

„Richtige“ Verschlüsselung am Beispiel eperi



Die wichtigsten Fakten: Verschlüsselung

- Vorteile:
  - Schlüssel liegt nicht bei Microsoft, vorgeschaltetes Verschlüsselungsgateway (On Premise, im weiteren Rechenzentrum)
  - Mail, Onedrive, Sharepoint, Teams etc. kann verschlüsselt werden
  - Vollständige Suchfunktion bleibt erhalten
  - Skalierbar
  - Ab 250 User über Dienstleister wie z.B. Telekom nutzbar (Stand 10.24)

Die wichtigsten Fakten: Verschlüsselung

- Nachteile:
  - Funktionen via Power BI können eingeschränkt sein
  - Eigene oder gehostete Infrastruktur erforderlich
  - Unter 250 User aktuell (Juni 2024) deutlich teurer als > 250 User
  - Aktuell der einzige Anbieter der eine solche Lösung anbietet

Technische und organisatorische Maßnahmen

Die wichtigsten Fakten: Kontrolle

SOFTWARE

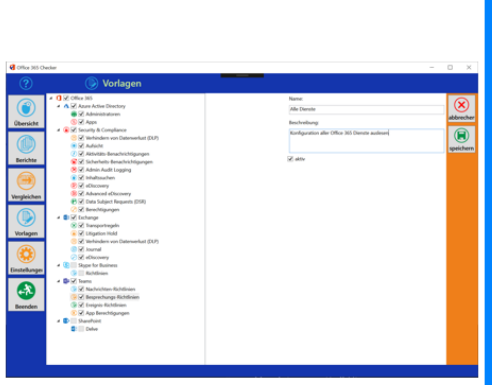
Microsoft 365 Checker

Behalten Sie die Konfiguration von Microsoft 365 unter Kontrolle!

Microsoft 365 bietet mit seinen zahlreichen Diensten eine Unmenge von Konfigurationsmöglichkeiten. Mit dem Microsoft 365 Checker können Sie die mitbestimmungsrelevanten Einstellungen auf einfache Weise auslesen. Auf Knopfdruck erstellen Sie entsprechende Berichte.

Und um Veränderungen festzustellen, vergleichen Sie die Berichte miteinander.

So können Sie auf einfache und schnelle Art und Weise feststellen, ob alle Einstellungen so sind, wie sie sein sollten.



Quelle: https://www.konverion.de/office_365_checker.html

Technische und organisatorische Maßnahmen

Die wichtigsten Fakten: Backup

- Microsoft 365 beinhaltet **KEINE** Backupverfahren. Microsoft garantiert NUR eine 24 x 7 x 365 Verfügbarkeit, das ist KEIN Backup!
- Ohne Backup z.B. keine Dateiwiederherstellung aus OneDrive
- Ohne Backup keine Sicherung der Mails
- Ohne Backup keine Sicherung des Sharepoints
- ……

MS Copilot

Microsoft Copilot, das Wichtigste vorab

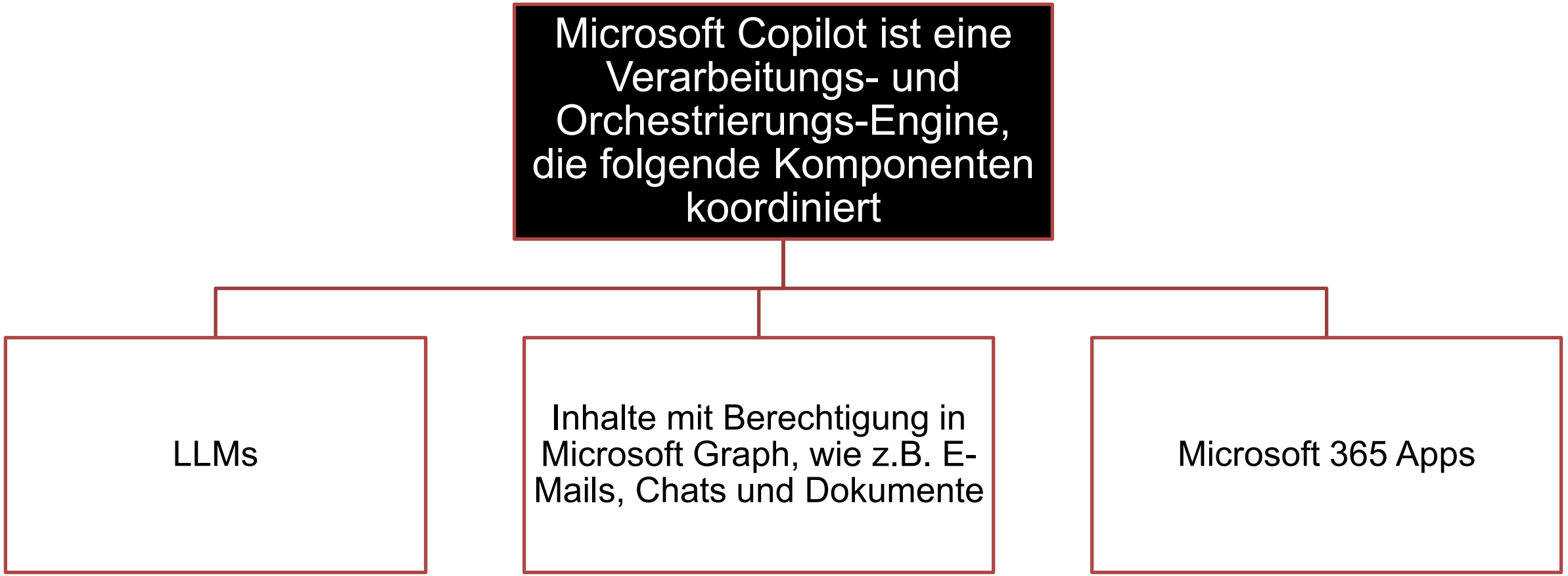
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Voraussetzung für die Nutzung ist Copilot Pro oder Copilot für Microsoft 365 Lizenz
- Alle Aktivitäten aus Copilot können vom Admin im Purview-Portal überwacht und überprüft werden
- Copilot verwendet eine Kombination aus LLMs, Deep Learning-Techniken und Datasets, um Inhalte zu verstehen, zusammenzufassen, vorherzusagen und zu generieren
- LLMs enthalten vortrainierte Modelle, z. B. Generative Pre-Trained Transformers (GPT) wie GPT-4

Quelle der Logos: Microsoft

Microsoft Copilot, das Wichtigste vorab

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



Microsoft Copilot, das Wichtigste vorab

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Copilot ist nicht gleich Copilot

Bing Copilot als Integration in Such-maschine

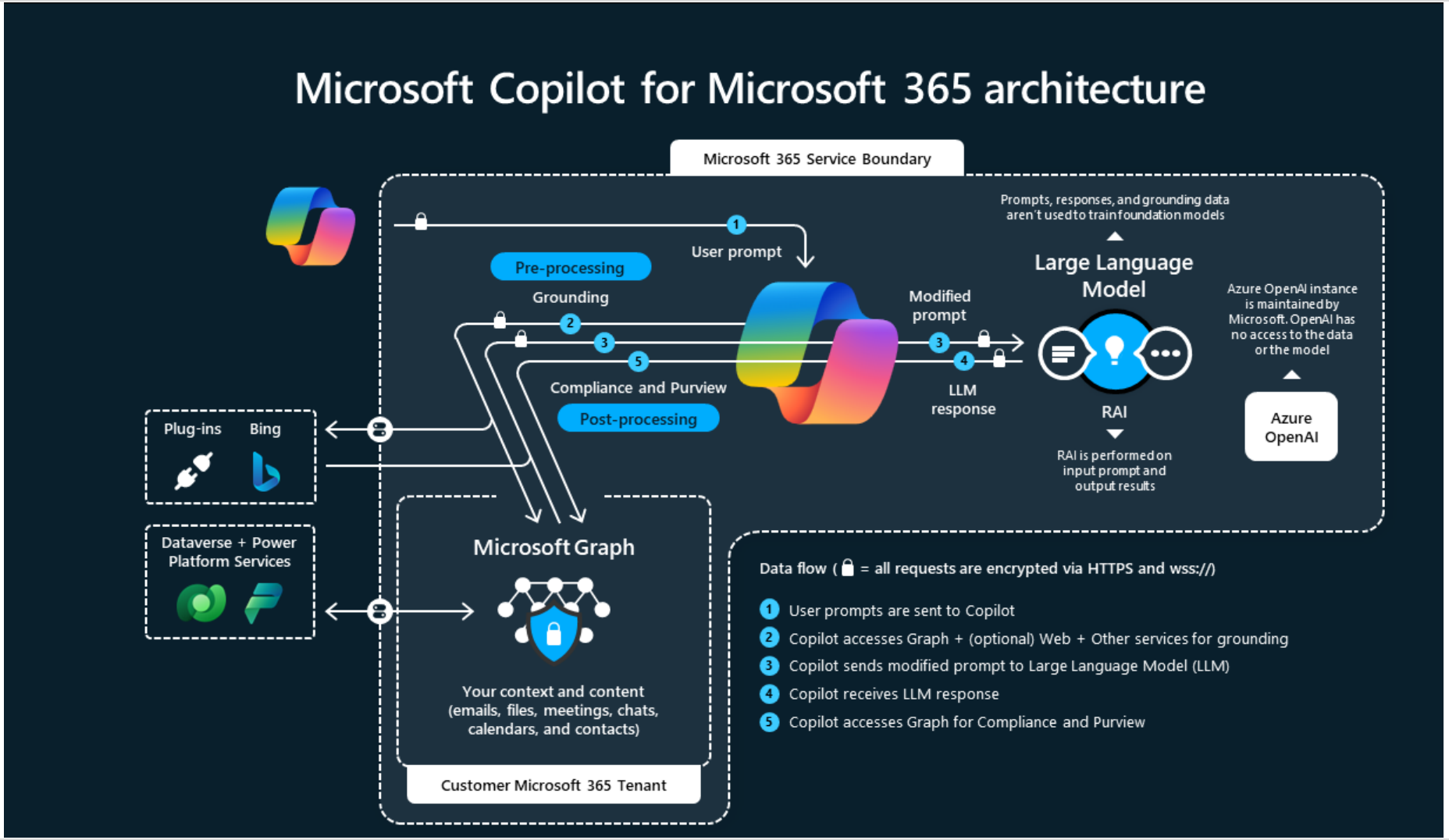
Copilot in Apps, z.B. Word, Excel, PowerPoint, Outlook

Copilot kann mit Plugins von Drittanbietern erweitert werden

Copilot in Microsoft 365 Online

Microsoft Copilot, das Wichtigste vorab

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



Microsoft Copilot, das Wichtigste vorab

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Microsoft 365-App	Feature	Beschreibung
Word	Entwurf mit Copilot	Generieren von Text mit und ohne Formatierung in neuen oder vorhandenen Dokumenten. Word-Dateien können auch zum Erden von Daten verwendet werden.
	Chat	Erstellen Sie Inhalte, fassen Sie zusammen, stellen Sie Fragen zu Ihrem Dokument, und führen Sie einfache Befehle über Chat aus.
PowerPoint	Entwurf mit Copilot	Erstellen Sie mithilfe von Unternehmensvorlagen eine neue Präsentation aus einer Eingabeaufforderung oder einer Word-Datei. PowerPoint-Dateien können auch zum Erden von Daten verwendet werden.
	Chat	Zusammenfassung und Q&A
	Leichte Befehle	Fügen Sie Folien und Bilder hinzu, oder nehmen Sie Überformatänderungen vor.

Microsoft Copilot,

Integriertes Abuse Monitoring-System und Content Filter

- **„Verbotene“ Kategorien:**
  - Hate, Sexual, Violence, Self-harm, Jailbreak risk, etc.
- **Funktionsweise**:

1. Inhaltsklassifizierung: Klassifizierungsmodelle erkennen verdächtige Inhalte in Prompts und Output
2. Missbrauchsmustererfassung: Algorithmen und Heuristiken analysieren die Nutzungsmuster, um potenziellen Missbrauch zu erkennen
3. Manuelle Kontrolle: „Human Review and Decision“ durch Mitarbeiter von MS
4. Ggf. Deaktivierung des Accounts durch MS: „Notification and Action“

Microsoft Copilot,

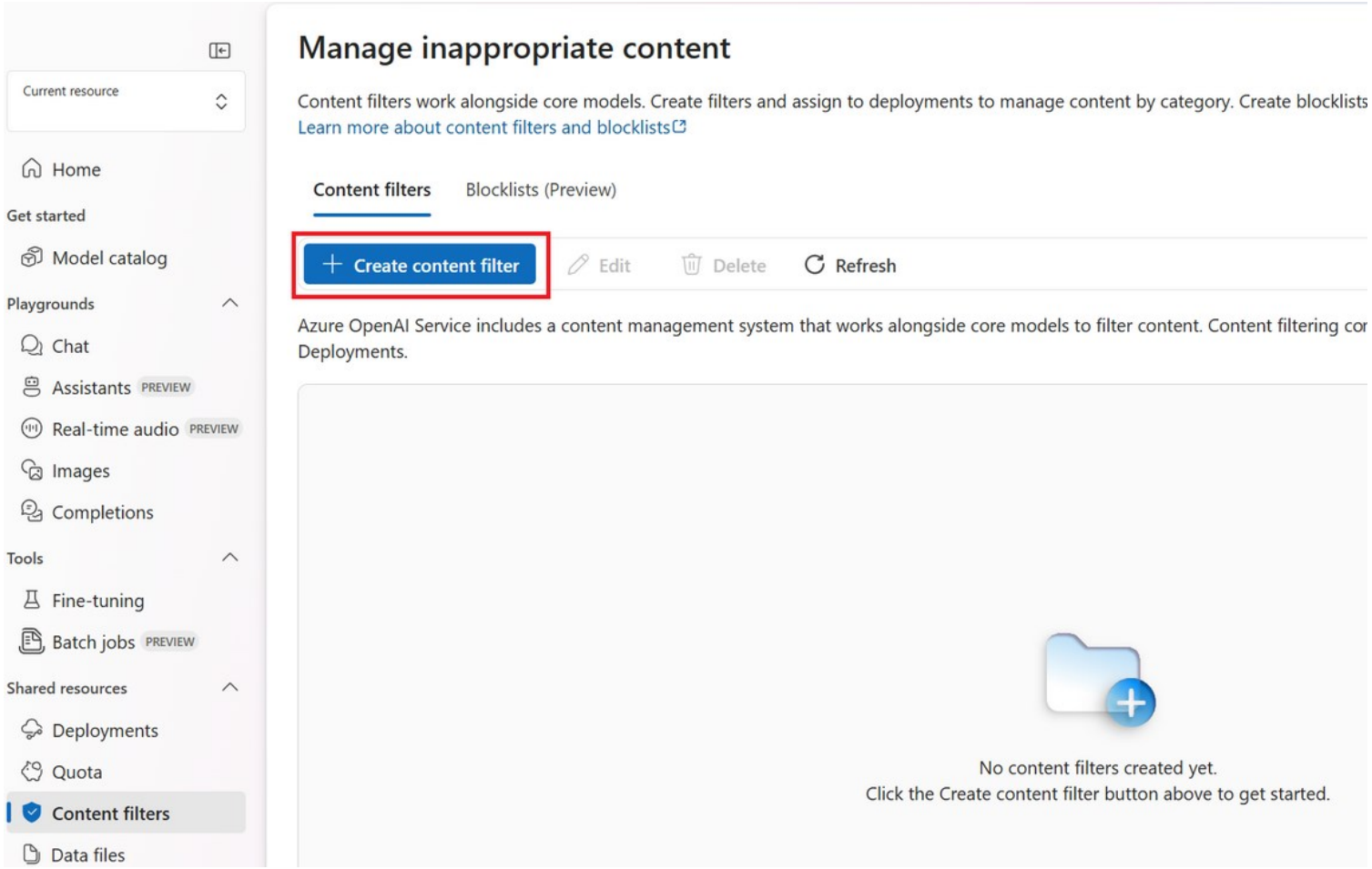
Integriertes Abuse Monitoring-System und Content Filter

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- **Verantwortlicher:**
  - Microsoft oder Kunde?
- **Rechtsgrundlage:**
  - Verhaltenskodex für KI-Dienste von Microsoft ???
- **Beschäftigtendatenschutz:**
  - Einbindung des Betriebsrates
  - Deaktivierung des Abuse Monitoring möglich, aber auch sinnvoll?
  - Informationspflichten gegenüber Beschäftigten

Microsoft Copilot
Content Filter zum Schutz vor Angriffen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



Fazit / ToDo‘s

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Ermitteln Sie die “Kronjuwelen“, was müssen Sie ggf. verschlüsseln, was nicht
- Wählen Sie das richtige Lizenzmodel
- Setzen Sie die technische Sicherheit bei Microsoft richtig um
- Überprüfen Sie die Einstellungen und Sicherheitsrichtlinien regelmäßig
- „Vermitteln Sie KI-Kompetenz (KI erkennen, verstehen und richtig einsetzen)“
- Erstellen / überarbeiten Sie entsprechende Sicherheits- und ggf. KI – Richtlinien


Questions?