# Rechtlicher Rahmen der Freigabe von Diensten in Shibboleth im Vergleich zur Freigabe von Drittdiensten in Microsoft 365

Johannes Nehlsen

# Agenda

- Rechtlicher Rahmen
- Aktuelles
- Attribute in Shibboleth
- Freigabe in EntraID
- Exkurs Microsoft 365 interne Dienste
- Beispiele
  - Edu-ID
  - ZoomX
  - Journal
- Entscheidungsempfehlungen

# Rechtlicher Rahmen

- Freigabe der Attribute
  - Meinung 1) Dienstefreigabe je nach Kategorie entweder Einwilligung, Aufgabenerfüllung oder berechtigte Interessen
  - Meinung 2) Freigabe erfolgt im Rahmen der gesetzlichen Aufgabenerfüllung
  - Sonderfall Serviceprovider ist Auftragsverarbeiter und Heimateinrichtung der Verantwortliche
- Arbeitshypothese IdP-Dienste einer Hochschule unterliegen nicht dem Data Act
- Alternative Perspektive
  - Freigabe als automatisierte Ausübung des Rechts auf Datenübertragbarkeit
- Sonderregelungen
  - OZG-Dienstleistungen
  - Pflichten als Registerbehörden

# Aktuelles

EuGH-Urteil vom 4. September 2025 C-413/23 P

- Nun eindeutig relativer Begriff der personenbezogenen Daten
- Perspektive des jeweiligen Verantwortlichen maßgeblich
- Für Empfänger können Daten, die für den Verantwortlichen pseudonym sind, selbst anonym sein
- Empfänger haben ggf. „Mittel“ oder Verarbeitungsprozesse mit Identifizierung, etwa KI-Systeme, Endgeräteinformationen, Support-Anfragen
- Verantwortlicher wird für die Offenlegung aus seiner Sicht eine Rechtsgrundlage oder Auftragsverarbeitung benötigen (umstritten)

➔ Werden keine identifizierenden Attribute übertragen und hat der Serviceprovider keine weiteren (legalen) Möglichkeiten zur Identifizierung, wird nun aus rechtlicher Sicht ein anonymer Dienst angeboten

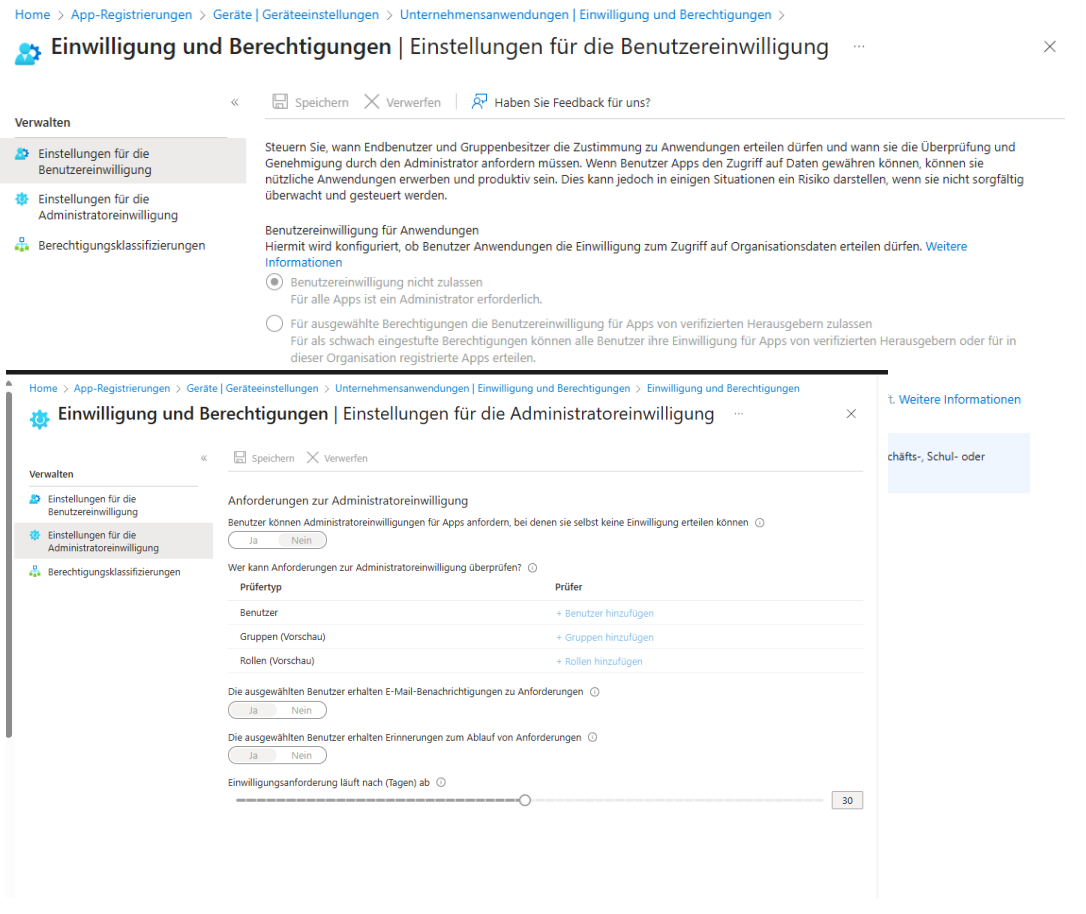
# Welche Informationen legt Shibboleth offen?

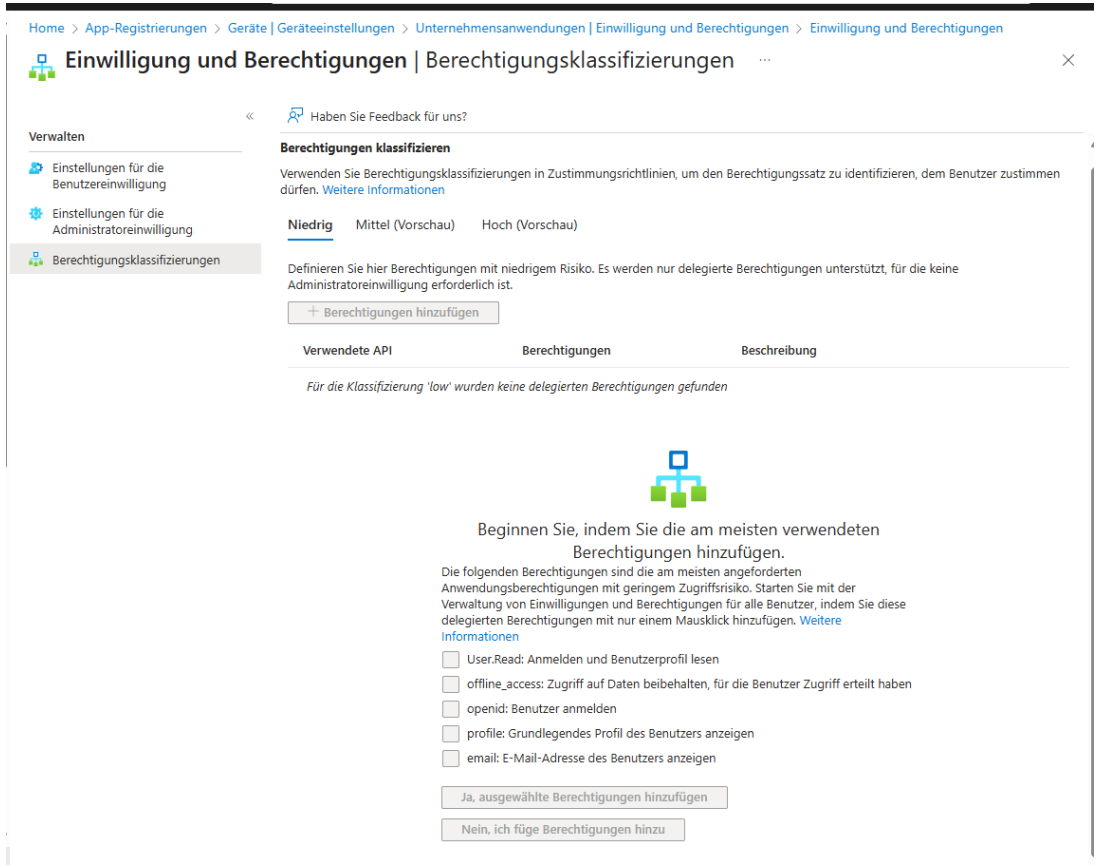
- Bekannte Attributfreigabe
- Proxydienste mit Informationsanreicherungen möglich
- Herausforderungen
  - Welche Serviceprovider möchte ich zulassen
  - Brauchen die Serviceprovider wirklich alle der angeforderten Attribute
  - Deprovisionierung
- Empfehlungen
  - Pseudonyme Daten können grundsätzlich freigegeben werden
    ➔ Ggf. Risiko von Tracking von Verlagen prüfen
  - Interner Prozess bei Freigabe für Attribute mit Personenbezug
    - Transparente Nutzungsbedingungen und Datenschutzinformationen
    - Code of Conduct

# Welche Informationen legt EntraID offen?

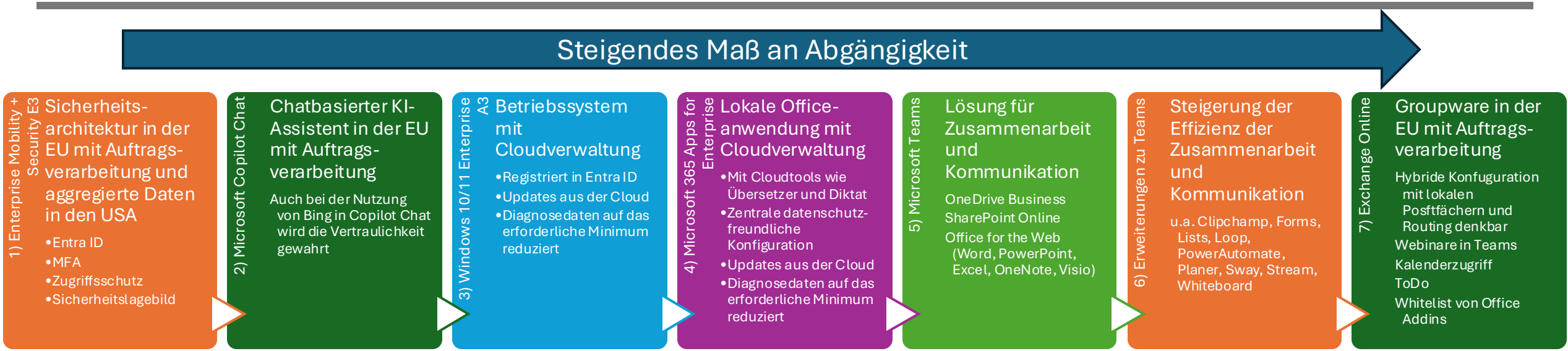
- Neben klassischen Attributen auch Zugriff auf die Graph API möglich
- Damit grundsätzlich Zugriff auf alle Dateien, auf die der Nutzer auch zugreifen kann (SharePoint Online / Teams / OneDrive Business)
- Herausforderungen
  - Anwendung und nicht nur der Nutzer ist berechtigt
  - Dateizugriff nur nach Nutzerinteraktion?
  - Deprovisionierung?
- Bewertung
  - Nach Risikobewertung passend zur Einrichtung konfigurieren

# Wie könnte man es gestalten?



# Kernelemente von Microsoft 365




Anmerkungen

- Ohne umstrittene Anwendungen wie Viva Insights, Dynamics 365
- Optional verbundene Erfahrungen
  - Alle Dienste haben zusätzlich weitere Addins mit Zugriff auf das Internet
    z.B.: Wetterdienst für Windows oder Outlook, Einfügen von YouTube in PowerPoint, Bildersuche in Bing auf Word, Thesaurus für Word, Suche in Wikipedia für Teams, Addins für Office
  - Diese Dienste sind ohne Auftragsverarbeitung und teilweise deaktiviert. Grundsätzlich könnten statt einer zentralen Deaktivierung auch die Entscheidung bei aufgeklärten Nutzern liegen.

# Edu-ID

Serviceprovider

- Erforderlichkeit der Attribute gut begründet
- Transparente Nutzungsbedingungen

Heimateinrichtungen

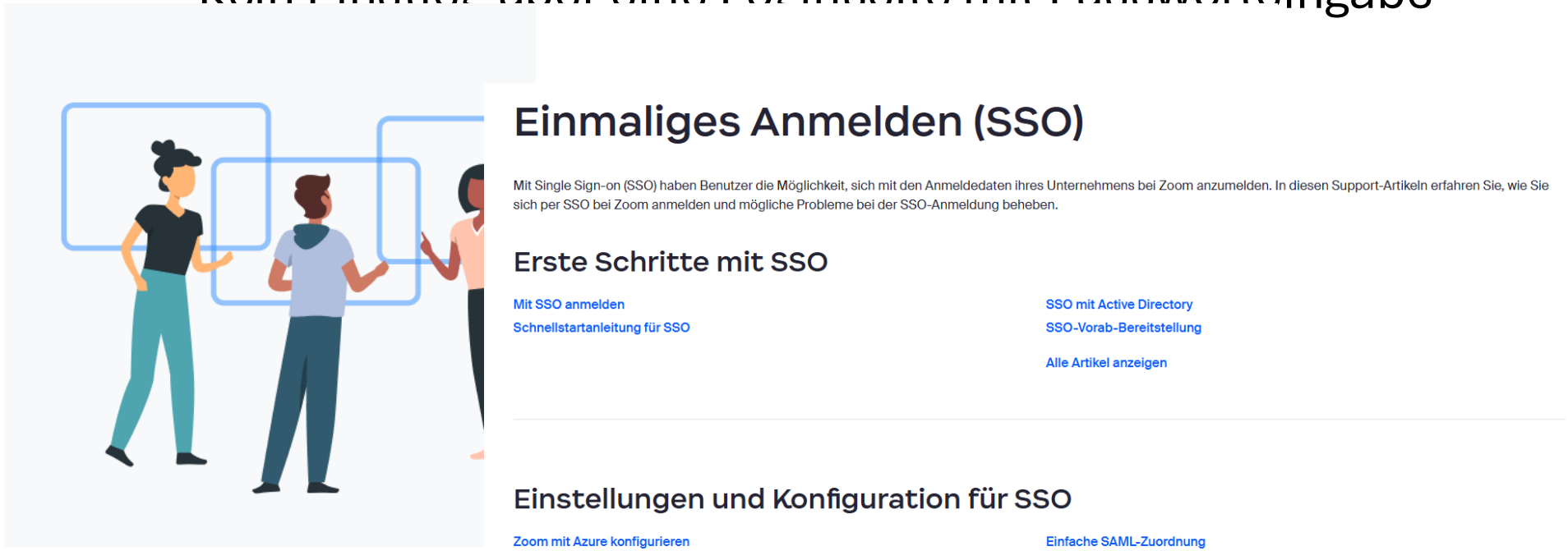
- Fortschreibung der internen Datenschutzdokumentation (Art. 30 Abs. 1 DSGVO), eine Aktualisierung der Datenschutzinformation (Art. 12-14 DSGVO) sowie der Risikobewertung (Art. 5, 24, 25, ggf. 35 DSGVO) also auch der TOM (Art. 32) erforderlich
- TOM verbessern, etwa Standardmaßnahmen nach OPS.1.1.2 Ordnungsgemäße IT-Administration nach IT-Grundschutzkompendium umsetzen

Was könnte der DFN noch besser machen?

- Löschfristen sind im Fließtext versteckt
- Empfänger noch etwas transparenter darstellbar

# Beispiel SSO bei Zoom X

- SSO als TOM
  - Kein Einstieg über eine Loginseite mit Passworteingabe



## Einmaliges Anmelden (SSO)

Mit Single Sign-on (SSO) haben Benutzer die Möglichkeit, sich mit den Anmeldedaten ihres Unternehmens bei Zoom anzumelden. In diesen Support-Artikeln erfahren Sie, wie Sie sich per SSO bei Zoom anmelden und mögliche Probleme bei der SSO-Anmeldung beheben.

### Erste Schritte mit SSO

Mit SSO anmelden
Schnellstartanleitung für SSO
SSO mit Active Directory
SSO-Vorab-Bereitstellung

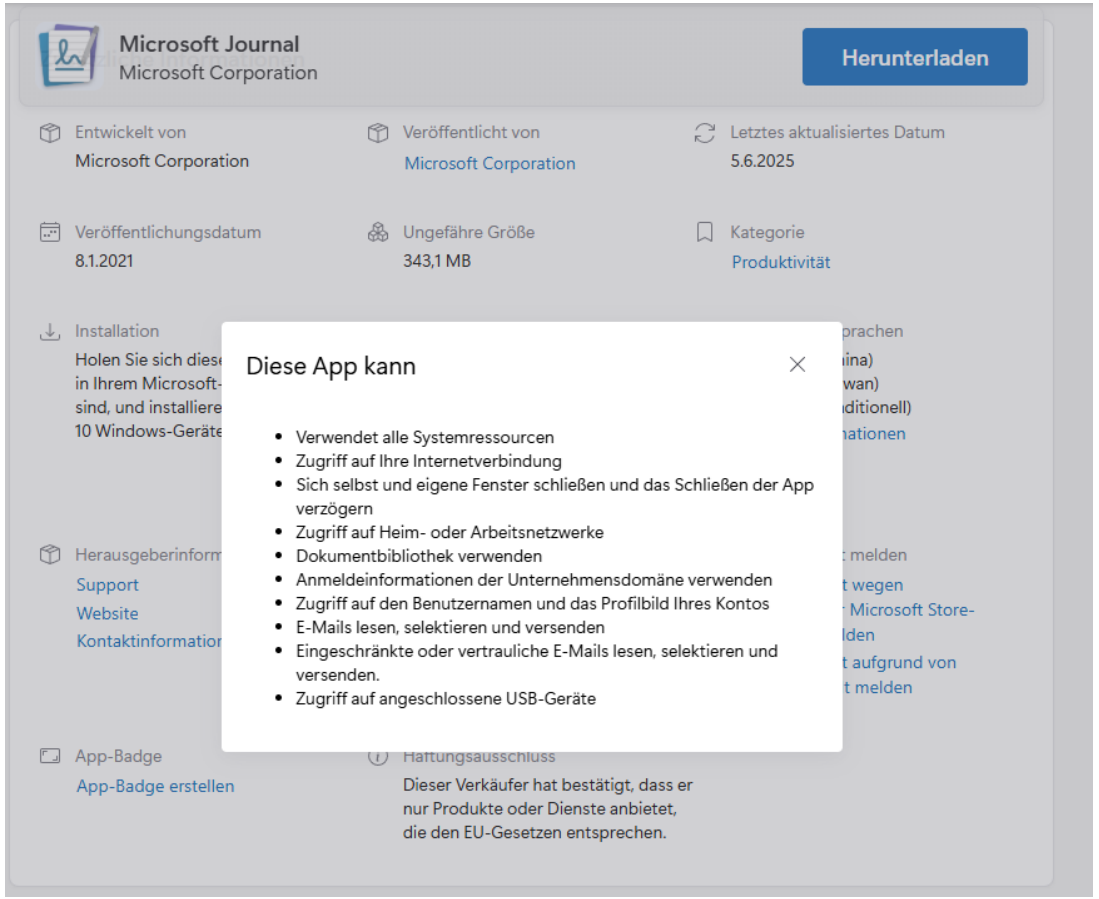
Alle Artikel anzeigen

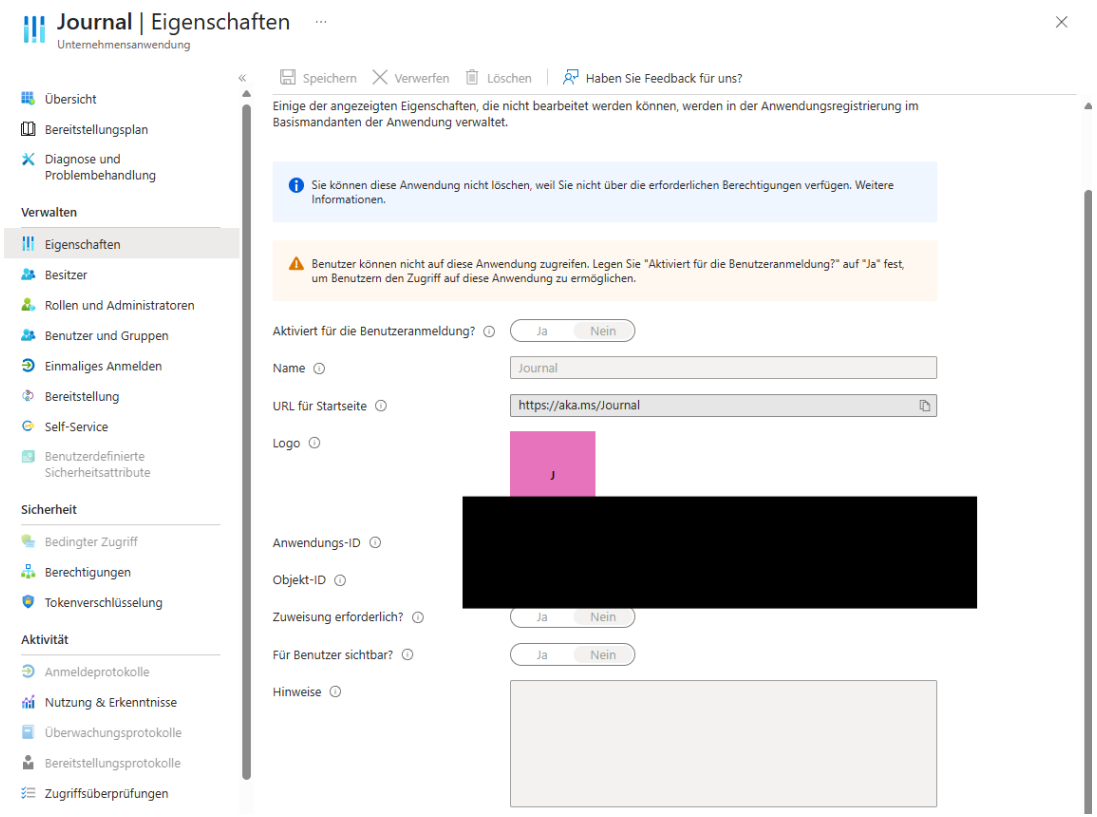
### Einstellungen und Konfiguration für SSO

Zoom mit Azure konfigurieren
Zoom SSO-Zertifikatswechsel
AD Sync to Zoom
Einfache SAML-Zuordnung
Zoom mit ADFS konfigurieren
Einrichten der erweiterten SAML-Zuordnung

Alle Artikel anzeigen

# Beispiel – Microsoft App Journal



# Journal - Bewertung

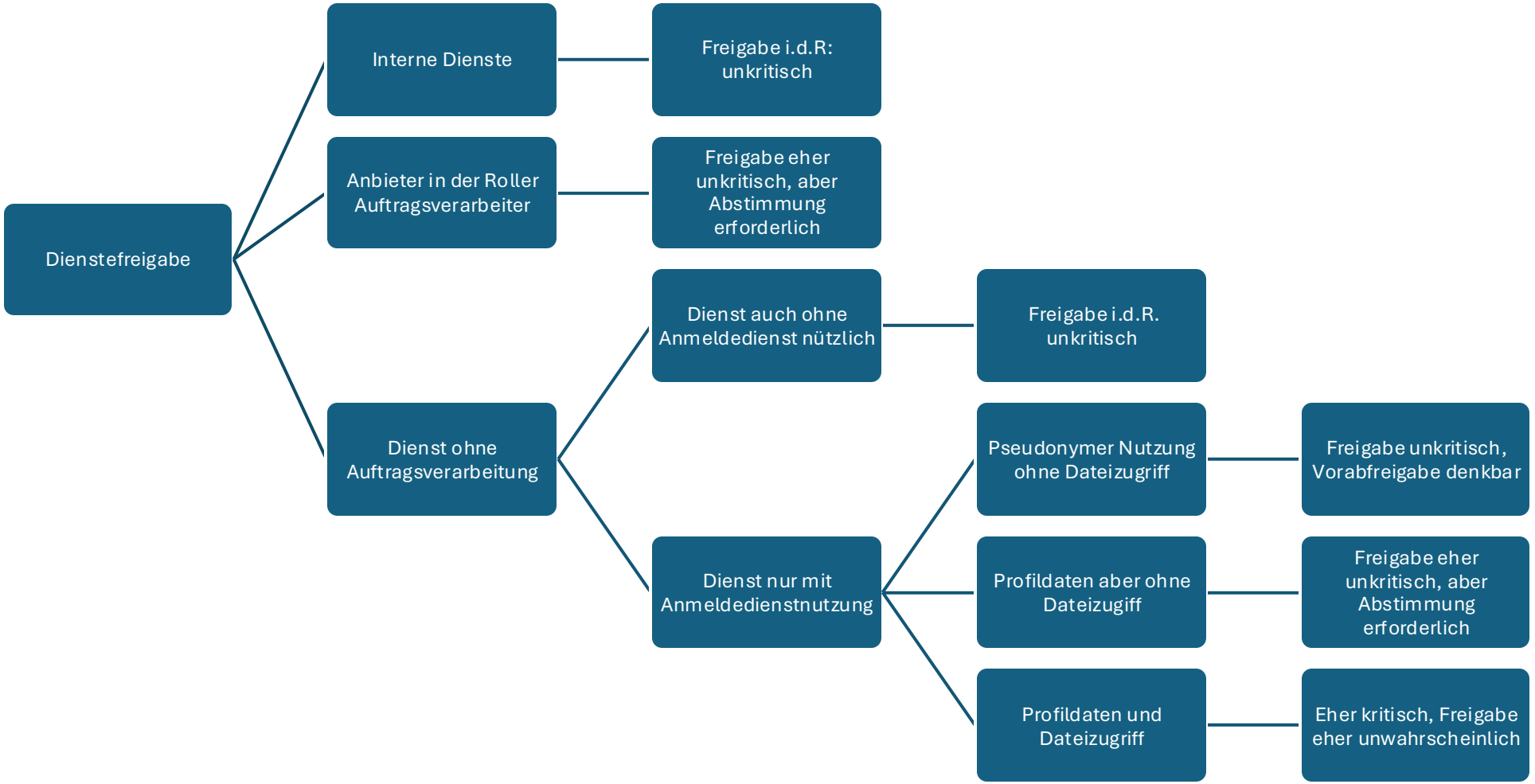
Prüfung

- Anwendung mit zahlreichen Zugriffsrechten
- Berechtigter Einsatzzweck
- Ausreichend klare Lizenzsituation
- Anbieter im Grundsatz vertrauenswürdig
- Anbieter nicht in der Rolle Auftragsverarbeiter für die Anwendung
- Ausreichende Pflege der Anwendung durch den Anbieter
- Risikovermeidung zur Blockierung der Nutzung des Logins in der App mit Entra

➔Beschränkter lokaler Einsatz

➔Keine Information zur Barrierefreiheit

# Entscheidungspfad



# Herzlichen Dank für Ihre Aufmerksamkeit!

Stabsstelle IT-Recht des

Digitalverbunds Bayern im Hochschulbereich

Johannes Nehlsen

Tel.: 0931/31-84217

johannes.nehlsen@uni-wuerzburg.de

it-recht@digitalverbund.bayern

https://www.rz.uni-wuerzburg.de/dienste/it-recht

Soziale Netzwerke meist mit Handle @JoNehlsen