

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



- Freigabe der Attribute
 - Meinung 1) Dienstfreigabe 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



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?



Home > App-Registrierungen > Geräte | Geräteeinstellungen > Unternehmensanwendungen | Einwilligung und Berechtigungen > Einwilligung und Berechtigungen

Einwilligung und Berechtigungen | Einstellungen für die Benutzereinwilligung

Verwalten

- Einstellungen für die Benutzereinwilligung
- Einstellungen für die Administratoreinwilligung
- Berechtigungsklassifizierungen

Speichern Verwerfen Haben Sie Feedback für uns?

Steuern Sie, wann Endbenutzer und Gruppenbesitzer die Zustimmung zu Anwendungen erteilen dürfen und wann sie die Überprüfung und Genehmigung durch den Administrator anfordern müssen. Wenn Benutzer Apps den Zugriff auf Daten gewähren können, können sie nützliche Anwendungen erwerben und produktiv sein. Dies kann jedoch in einigen Situationen ein Risiko darstellen, wenn sie nicht sorgfältig überwacht und gesteuert werden.

Benutzereinwilligung für Anwendungen
Hiermit wird konfiguriert, ob Benutzer Anwendungen die Einwilligung zum Zugriff auf Organisationsdaten erteilen dürfen. [Weitere Informationen](#)

- Benutzereinwilligung nicht zulassen
Für alle Apps ist ein Administrator erforderlich.
- Für ausgewählte Berechtigungen die Benutzereinwilligung für Apps von verifizierten Herausgebern zulassen
Für als schwach eingestufte Berechtigungen können alle Benutzer ihre Einwilligung für Apps von verifizierten Herausgebern oder für in dieser Organisation registrierte Apps erteilen.

Home > App-Registrierungen > Geräte | Geräteeinstellungen > Unternehmensanwendungen | Einwilligung und Berechtigungen > Einwilligung und Berechtigungen

Einwilligung und Berechtigungen | Einstellungen für die Administratoreinwilligung

Verwalten

- Einstellungen für die Benutzereinwilligung
- Einstellungen für die Administratoreinwilligung
- Berechtigungsklassifizierungen

Speichern Verwerfen

Anforderungen zur Administratoreinwilligung
Benutzer können Administratoreinwilligungen für Apps anfordern, bei denen sie selbst keine Einwilligung erteilen können

Ja Nein

Wer kann Anforderungen zur Administratoreinwilligung überprüfen?

Prüfertyp	Prüfer
Benutzer	+ Benutzer hinzufügen
Gruppen (Vorschau)	+ Gruppen hinzufügen
Rollen (Vorschau)	+ Rollen hinzufügen

Die ausgewählten Benutzer erhalten E-Mail-Benachrichtigungen zu Anforderungen

Ja Nein

Die ausgewählten Benutzer erhalten Erinnerungen zum Ablauf von Anforderungen

Ja Nein

Einwilligungsanforderung läuft nach (Tagen) ab

Home > App-Registrierungen > Geräte | Geräteeinstellungen > Unternehmensanwendungen | Einwilligung und Berechtigungen > Einwilligung und Berechtigungen

Einwilligung und Berechtigungen | Berechtigungsklassifizierungen

Verwalten

- Einstellungen für die Benutzereinwilligung
- Einstellungen für die Administratoreinwilligung
- Berechtigungsklassifizierungen

Haben Sie Feedback für uns?

Berechtigungen klassifizieren
Verwenden Sie Berechtigungsklassifizierungen in Zustimmungsrichtlinien, um den Berechtigungssatz zu identifizieren, dem Benutzer zustimmen dürfen. [Weitere Informationen](#)

Niedrig Mittel (Vorschau) Hoch (Vorschau)

Definieren Sie hier Berechtigungen mit niedrigem Risiko. Es werden nur delegierte Berechtigungen unterstützt, für die keine Administratoreinwilligung erforderlich ist.

+ Berechtigungen hinzufügen

Verwendete API	Berechtigungen	Beschreibung
Für die Klassifizierung 'low' wurden keine delegierten Berechtigungen gefunden		

Beginnen Sie, indem Sie die am meisten verwendeten Berechtigungen hinzufügen.

Die folgenden Berechtigungen sind die am meisten angeforderten Anwendungsberechtigungen mit geringem Zugriffsrisiko. Starten Sie mit der Verwaltung von Einwilligungen und Berechtigungen für alle Benutzer, indem Sie diese delegierten Berechtigungen mit nur einem Mausklick hinzufügen. [Weitere Informationen](#)

- User.Read: Anmelden und Benutzerprofil lesen
- offline_access: Zugriff auf Daten beibehalten, für die Benutzer Zugriff erteilt haben
- openid: Benutzer anmelden
- profile: Grundlegendes Profil des Benutzers anzeigen
- email: E-Mail-Adresse des Benutzers anzeigen

Ja, ausgewählte Berechtigungen hinzufügen

Nein, ich füge Berechtigungen hinzu

Kernelemente von Microsoft 365



Steigendes Maß an Abgängigkeit



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.



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 Finstiege 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



Microsoft Journal
Microsoft Corporation

Herunterladen

Entwickelt von: Microsoft Corporation
Veröffentlicht von: Microsoft Corporation
Letztes aktualisiertes Datum: 5.6.2025

Veröffentlichungsdatum: 8.1.2021
Ungefähre Größe: 343,1 MB
Kategorie: Produktivität

Diese App kann

- Verwendet alle Systemressourcen
- Zugriff auf Ihre Internetverbindung
- Sich selbst und eigene Fenster schließen und das Schließen der App verzögern
- Zugriff auf Heim- oder Arbeitsnetzwerke
- Dokumentbibliothek verwenden
- Anmeldeinformationen der Unternehmensdomäne verwenden
- Zugriff auf den Benutzernamen und das Profilbild Ihres Kontos
- E-Mails lesen, selektieren und versenden
- Eingeschränkte oder vertrauliche E-Mails lesen, selektieren und versenden.
- Zugriff auf angeschlossene USB-Geräte

Journal | Eigenschaften
Unternehmensanwendung

Übersicht
Bereitstellungsplan
Diagnose und Problembehandlung

Verwalten
Eigenschaften
Besitzer
Rollen und Administratoren
Benutzer und Gruppen
Einmaliges Anmelden
Bereitstellung
Self-Service
Benutzerdefinierte Sicherheitsattribute

Sicherheit
Bedingter Zugriff
Berechtigungen
Tokenverschlüsselung

Aktivität
Anmeldeprotokolle
Nutzung & Erkenntnisse
Überwachungsprotokolle
Bereitstellungsprotokolle
Zugriffsüberprüfungen

Einige der angezeigten Eigenschaften, die nicht bearbeitet werden können, werden in der Anwendungsregistrierung im Basismandanten der Anwendung verwaltet.

Sie können diese Anwendung nicht löschen, weil Sie nicht über die erforderlichen Berechtigungen verfügen. Weitere Informationen.

Benutzer können nicht auf diese Anwendung zugreifen. Legen Sie "Aktiviert für die Benutzeranmeldung?" auf "Ja" fest, um Benutzern den Zugriff auf diese Anwendung zu ermöglichen.

Aktiviert für die Benutzeranmeldung? Ja Nein

Name

URL für Startseite

Logo

Anwendungs-ID

Objekt-ID

Zuweisung erforderlich? Ja Nein

Für Benutzer sichtbar? Ja Nein

Hinweise

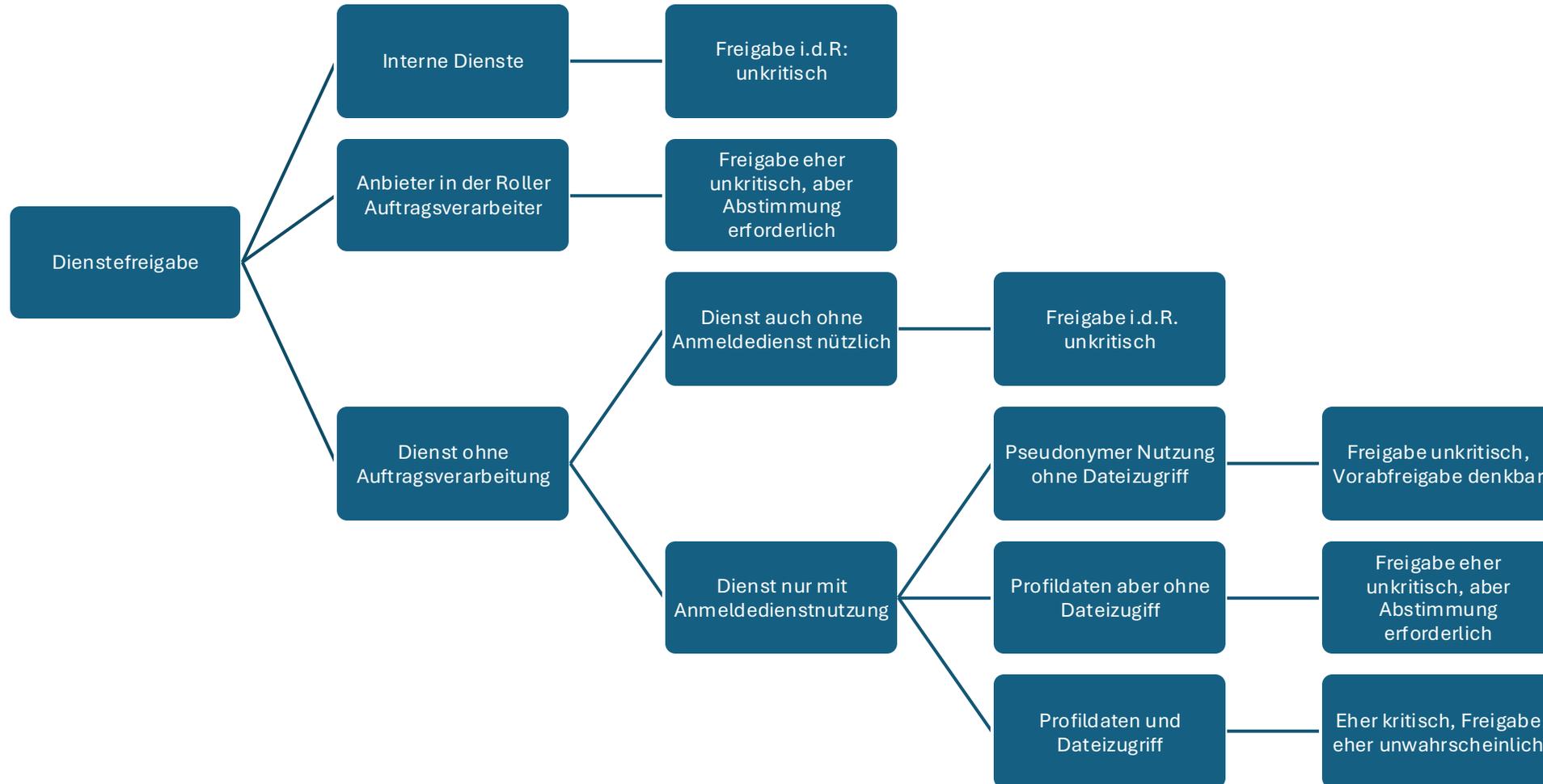
Journal - Bewertung



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



Dieses Werk ohne Zitate, geschützte Marken, Icons und unwesentlichem Beiwerk ist lizenziert unter einer [Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](https://creativecommons.org/licenses/by-sa/4.0/).