Hintergrund zu den Berechtigungen im OCC

ONLINE COMPLIANCE CENTER
powered by **sitaas GmbH**

Mit diesem begleitenden Dokument erläutern wir die Berechtigungen, die im Zuge der neuen Technologie zur Nutzung der Backup- und Restore Funktion des Online Compliance Centers von unseren Kunden bestätigt werden müssen.

Der **Exchange Connector** benötigt Zugriff auf ausgewählte Postfach- und Kalenderdaten, um:

- E-Mails automatisiert zu verarbeiten (Lesen/Schreiben)
- Ordnerstrukturen in Postfächern auszulesen
- Kalenderdaten zu lesen und Termine zu erstellen

Übersicht der Berechtigungen:

- Calendars.ReadWrite → Kann Kalender aller Benutzer lesen und Termine erstellen/ändern.
- MailboxFolder.Read.All → Kann alle Ordner in Benutzerpostfächern sehen (z. B. Posteingang, Gesendet), aber keine E-Mails darin lesen.
- MailboxFolder.ReadWrite.All → Kann Ordner in Benutzerpostfächern lesen, erstellen, umbenennen und verschieben.
- Mail.Read → Kann vollständige E-Mails eines Benutzers lesen (Inhalt + Anhänge).
- Mail.ReadBasic → Kann nur Basisinformationen von E-Mails eines Benutzers lesen (Betreff, Absender, Zeit).
- Mail.ReadWrite → Kann vollständige E-Mails lesen, erstellen, ändern oder verschieben.
- MailboxSettings.Read → Kann Postfacheinstellungen lesen (z. B. Sprache, Zeitzone, Signaturen).
- MailboxSettings.ReadWrite → Kann Postfacheinstellungen lesen und ändern.

Die **Microsoft Teams**-Berechtigungen betreffen hauptsächlich den Zugriff auf Teams, Kanäle und Nachrichten.

Übersicht der Berechtigungen:

- Create channels → Erlaubt das Erstellen neuer Kanäle in Microsoft Teams.
- Read the names and descriptions of all channels → Ermöglicht das Auslesen der Namen und Beschreibungen aller Kanäle in einem Team.
- Read the members of all channels → Gibt Zugriff auf die Liste aller Mitglieder eines Kanals.
- Alle Kanalnachrichten lesen (Read all channel messages) → Berechtigt den Zugriff auf sämtliche Nachrichten innerhalb aller Kanäle in einem Team.
- Read the names, descriptions, and settings of all channels → Erlaubt das Abrufen von Kanalnamen, Beschreibungen und den Einstellungen der Kanäle.

Hintergrund zu den Berechtigungen im OCC

ONLINE COMPLIANCE CENTER
powered by **sitaas GmbH**

- Read and write the names, descriptions, and settings of all channels → Erlaubt das Lesen und Ändern der Kanalnamen, Beschreibungen und Einstellungen.
- Create chats → Ermöglicht das Erstellen neuer Chat-Nachrichten in Microsoft Teams.
- Alle Chatnachrichten lesen (Read all chat messages) → Gibt vollständigen Zugriff auf alle privaten und Gruppen-Chats in Microsoft Teams.
- Verzeichnisdaten lesen (Read directory data) → Erlaubt den Zugriff auf das gesamte Azure AD-Verzeichnis (z. B. Benutzer, Gruppen, Rollen).

Die nachfolgenden Berechtigungen beziehen sich auf die Organisation und Verwaltung von Teams und Benutzern.

- Read your organization's policies → Erlaubt das Lesen der Unternehmensrichtlinien, z. B. Sicherheits- und Compliance-Regeln.
- Get a list of all teams → Ruft eine Liste aller Teams in der Organisation ab.
- Add and remove members from all teams → Erlaubt das Hinzufügen und Entfernen von Mitgliedern in allen Teams.
- Create chat and channel messages with anyone's identity and with any timestamp → Erlaubt das Erstellen von Nachrichten in Chats und Kanälen, indem eine beliebige Identität oder ein beliebiger Zeitstempel verwendet wird.
- Vollständige Profile aller Benutzer lesen (Read full profiles of all users) → Erlaubt den Zugriff auf vollständige Benutzerprofile im Azure AD (einschließlich E-Mail, Name, Rolle).
- Anmelden und Benutzerprofil lesen (Sign in and read user profile)
- → Erlaubt es, sich im Namen eines Benutzers anzumelden und dessen Profilinformationen auszulesen.

Die Microsoft SharePoint- und OneDrive-Berechtigungen betreffen die Verwaltung und den Zugriff auf Dateien und Listen in SharePoint-Online und OneDrive.

Übersicht der Berechtigungen:

- Dateien in allen Websitesammlungen lesen (Read files in all site collections) → Erlaubt das Lesen aller Dateien innerhalb aller SharePoint-Websitesammlungen und OneDrive.
- Dateien in allen Websitesammlungen lesen und schreiben (Read and write files in all site collections) → Wie oben, aber zusätzlich mit Schreibrechten für Dateien.
- Elemente und Listen in allen Websitesammlungen erstellen, bearbeiten und löschen → Erlaubt das Erstellen, Ändern und Löschen von Listenelementen (z. B. SharePoint-Listen und Bibliotheken).

Hintergrund zu den Berechtigungen im OCC

- Elemente in allen Websitesammlungen lesen (Vorschau) (Read items in all site collections - Preview) → Experimentelle (Vorschau-)Berechtigung, um Listenelemente innerhalb aller SharePoint-Websites zu lesen.
- Verfügt über Vollzugriff auf alle Sitesammlungen (Full control of all site collections) → Gewährt vollständige Kontrolle über alle SharePoint- und OneDrive-Websites.

Darüber hinaus benötigt es Berechtigungen im Bereich Azure Information Protection & Sicherheit. Diese betreffen den Zugriff auf geschützte Inhalte und Sicherheitsrichtlinien.

- Read all service configuration and log data for the Azure Information Protection service → Gibt Zugriff auf die Azure Information Protection (AIP) Konfigurationen und Logs (z. B. für Data Loss Prevention und Verschlüsselung).
- Create protected content → Erlaubt das Erstellen von geschützten Inhalten, z. B. durch Microsoft Information Protection Labels.
- Read all protected content for this tenant → Gibt Zugriff auf alle geschützten Inhalte im gesamten Mandanten (z. B. verschlüsselte Dateien und E-Mails).
- Read protected content on behalf of a user → Erlaubt das Lesen geschützter Inhalte, wenn ein Benutzer dies genehmigt.
- Create protected content on behalf of a user → Erlaubt das Erstellen von geschützten Dokumenten und E-Mails im Namen eines Benutzers.
- Read all unified policies of the tenant → Gibt Zugriff auf alle einheitlichen Sicherheits- und Compliance-Richtlinien in Microsoft 365.