

Broszura techniczna dla Usługi „Engagy360”

Jak jest hostowana usługa Engagy360?

Usługa Engagy360 jest dostępna w modelu SaaS (Software-as-a-Service), co oznacza, że centralna część usługi jest hostowana po stronie dostawcy. W infrastrukturze klienta konieczne jest jedynie skonfigurowanie uprawnień oraz zainstalowanie aplikacji SPFx w środowisku SharePoint i Teams.

Gdzie są przechowywane dane?

Zasób	Lokalizacja	Uwagi
Azure SQL	West Europe	Informacja o licencji, informacja o środowisku SharePoint klienta, informacja o portalach i witrynach, szablonach witryn, zadania redaktorów, raporty metryk witryn, informacje o powiadomieniach.
Azure Storage Account (Tables)	Lokalizacje na terenie UE	Informacje o operacjach wykonywanych w środowisku klienta takie jak instalacje/aktualizacje aplikacji SharePoint.
Azure Storage Account (Blob containers)	Lokalizacje na terenie UE	Pliki graficzne używane do wygenerowania motywów graficznych przez klientów usługi. Pliki danych źródłowych przekazane przez klientów w procesie generowania portalu.
Azure Application Insights	West Europe	Logi usługi
Azure Key Vault	West Europe	Operacje w środowisku klienta wykonywane są w imieniu użytkownika, tokeny dostępowe użytkownika są przechowywane w usłudze Azure Key Vault.
Azure Open AI	Sweden Central	Zapytania i wygenerowane odpowiedzi mechanizmów open AI są przechowywane na potrzeby zapobiegania nadużyciom i generowaniu szkodliwych treści. Dane nie są udostępniane innym usługom, nie są wykorzystywane do uczenia modeli OpenAI i Azure OpenAI. Szczegółowy opis bezpieczeństwa informacji Azure Open AI: https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy .

Jakich uprawnień wymaga usługa?

1. Uprawnienia wymagane do konfiguracji usługi (administrator usługi):
 - Globalny administrator



- Administrator SharePoint

2. Aplikacje Azure AD

Aplikacja	Opis	Rodzaj uprawnień
Engagy360 Cloud Control Panel	Aplikacja obsługująca działanie Panelu Administracyjnego.	• Microsoft Graph ◦ User.Read (Delegated) ◦ User.Read.All (Delegated) ◦ Group.Read.All (Delegated) ◦ Sites.Read.All (Delegated) • Office 365 SharePoint Online ◦ AllSites.FullControl (Delegated) • Engagy360 Service ◦ user_impersonation
Engagy360 Service	Aplikacja obsługująca operacje web api usługi Engagy360.	• Microsoft Graph ◦ Group.Read.All (Application) ◦ Sites.Read.All (Application) ◦ TeamsActivity.Send (Application) ◦ User.Read (Delegated) ◦ User.Read.All (Application) ◦ Application.Read.All (Delegated) ◦ DelegatedPermissionGrant.ReadWrite.All (Delegated) ◦ Community.ReadWrite (Application) ◦ SharePointTenantSettings.Read.All (Application) ◦ AppCatalog.Read.All • Office 365 SharePoint Online ◦ Sites.FullControl.All (Application) ◦ Sites.Selected (Application) ◦ AllSites.FullControl.All (Delegated)
Engagy360 EngagyApp	Aplikacja obsługująca logowanie w aplikacji mobilnej i dostępie webowym modułu EngagyApp.	• Engagy360 Service ◦ user_impersonation

3. Aplikacje SPFx

Aplikacja	Opis	Rodzaj uprawnień
-----------	------	------------------



Engagy360	Aplikacja kliencka usługi Engagy360 działająca w środowisku SharePoint i Teams.	- Microsoft Graph - User.Read (Delegated) - User.Read.All (Delegated) - Group.Read.All (Delegated) - Engagy360 Service - user_impersonation
-----------	---	--

4. Przykładowe wykorzystanie poszczególnych uprawnień

Aplikacja Entra ID	Usługa	Zakres uprawnień	Rodzaj uprawnień	Wykorzystanie
Engagy360 Cloud Control Panel	Microsoft Graph	Group.Read.All	Delegacyjne	Edycja/dodawanie witryny/portalu
Engagy360 Cloud Control Panel	Microsoft Graph	Sites.Read.All	Delegacyjne	Ustalenie adresu SharePoint dla tenanta
Engagy360 Cloud Control Panel	Microsoft Graph	User.Read	Delegacyjne	Pobranie informacji o zalogowanym użytkowniku (m.in. kontrolka zalogowanego użytkownika)
Engagy360 Cloud Control Panel	Microsoft Graph	User.Read.All	Delegacyjne	Edycja/dodawanie witryny/portalu
Engagy360 Cloud Control Panel	SharePoint	AllSites.FullControl	Delegacyjne	- Tworzenie portalu/witryny - Dodawanie istniejącego portalu/witryny - Weryfikacja uprawnień użytkownika
Engagy360 Cloud Control Panel	Engagy360 Service	user_impersonation	Delegacyjne	Komunikacja z WebAPI usługi Engagy360
Engagy360 Service	Microsoft Graph	Group.Read.All	Aplikacyjne	- Wysyłanie powiadomień Teams - Wykonanie raportu ScoreCard
Engagy360 Service	Microsoft Graph	Sites.Read.All	Aplikacyjne	Wykonanie raportu ScoreCard
Engagy360 Service	Microsoft Graph	TeamsActivity.Send	Aplikacyjne	Wysyłanie powiadomień Teams
Engagy360 Service	Microsoft Graph	User.Read	Delegacyjne	Weryfikacja licencji Microsoft 365 (wysyłka powiadomień Teams)

Engagy360 Service	Microsoft Graph	User.Read.All	Aplikacyjne	- Wysyłanie powiadomień Teams - Tworzenie portalu z szablonu (nadawanie uprawnień) - Wnioski do dodanie/utworzenie witryny (wysyłanie powiadomień) - Sprawdzanie uprawnień użytkownika
Engagy360 Service	Microsoft Graph	Application.Read.All	Delegacyjne	Sprawdzenie uprawnień aplikacji SharePoint Online Client Extensibility Web Application Principal
Engagy360 Service	Microsoft Graph	DelegatedPermissionsGrant.ReadWrite.All	Delegacyjne	Zatwierdzanie uprawnień aplikacji SPFx (SharePoint Online Client Extensibility Web Application Principal).
Engagy360 Service	Microsoft Graph	Community.ReadWrite.All	Aplikacyjne	Odczyt i tworzenie społeczności Viva Engage
Engagy360 Service	Microsoft Graph	SharePointTenantSettings.Read.All	Aplikacyjne	Tworzenie witryn (sprawdzenie czy użytkownicy mogą tworzyć witryny)
Engagy360 Service	Microsoft Graph	AppCatalog.Read.All	Aplikacyjne	Sprawdzenie statusu instalacji aplikacji Engagy360 w Teams
Engagy360 Service	SharePoint	Sites.FullControl.All	Aplikacyjne	- Ustawianie identyfikatorów śledzenia - Tworzenie witryny z szablonu (zastosowanie szablonu) - Akceptacja tworzenia witryny z szablonu (zastosowanie szablonu) - Wykonanie raportu ScoreCard - Odpinanie witryny z usługi Engagy360 (usuwanie identyfikatorów śledzenia) - Sprawdzanie uprawnień użytkowników witrynach SharePoint - Podłączanie witryn do witryn centrum (tworzenie witryny)
Engagy360 Service	SharePoint	Sites.Selected	Aplikacyjne	Wykorzystywane w wariacie wdrożenia na obniżonych uprawnieniach



				Wykorzystywane na witrynach: • uprawnienie na poziomie read (odczyt) na witrynie centralnej administracji; to uprawnienie pozwoli przeczytać listę wszystkich witryn, ale nie pozwoli na sprawdzenie zawartości innych witryn, ani na skonfigurowanie sobie dostępu do innych witryn. • uprawnienie na poziomie fullControl (pełna kontrola) na witrynach podłączonych do usługi Engagy360
Engagy360 Service	SharePoint	AllSites.FullControl	Delegacyjne	• Tworzenie portalu z szablonu • Tworzenie witryny z szablonu (tworzenie witryny) • Akceptacja tworzenia witryny z szablonu • Odpinanie witryny z usługi Engagy360 (odpinanie od witryny centrum) • Instalacja aplikacji SPFx
SharePoint Online Client Extensibility Web Application Principal	Microsoft Graph	User.Read	Delegacyjne	• Pobranie informacji o zalogowanym użytkowniku
SharePoint Online Client Extensibility Web Application Principal	Microsoft Graph	User.Read.All	Delegacyjne	• Odczyt wszystkich użytkowników m.in. w komponencie książki adresowej
SharePoint Online Client Extensibility Web Application Principal	Microsoft Graph	Group.Read.All	Delegacyjne	• Odczyt wszystkich grup m.in. funkcjonalności subskrypcji na stronach
SharePoint Online Client Extensibility Web Application Principal	Engagy360 Service	user_impersonation	Delegacyjne	• Komunikacja z WebAPI usługi Engagy360

5. Tryb obniżonych uprawnień

Domyślnie usługa Engagy360 korzysta z uprawnień aplikacyjnych o poziomie *FullControl* w całej platformie SharePoint klienta. Alternatywnie aplikacja może działać w trybie obniżonych uprawnień, wykorzystując jedynie uprawnienie aplikacyjne *Sites.Selected*. W tym trybie wymagane są:

- uprawnienia *Read* do witryny administracyjnej SharePoint,
- uprawnienia *FullControl* do poszczególnych witryn zarejestrowanych w usłudze.

Uprawnienia te są nadawane w trakcie:

- rejestracji środowiska klienta (na witrynie administracyjnej),
- rejestracji poszczególnych witryn w usłudze.

Aplikacja automatycznie przechodzi w tryb obniżonych uprawnień, jeśli uprawnienia *FullControl* zostaną jej odebrane w Entra ID.

W tym trybie zakres dostępnych operacji może ulec ograniczeniom, ponieważ aplikacja musi działać wyłącznie w granicach uprawnień bieżącego użytkownika — szczególnie w przypadku operacji na witrynach niezarejestrowanych w usłudze lub podczas tworzenia nowych witryn.

Dane osobowe w usłudze Engagy360

Przechowywanie danych osobowych

Rodzaj informacji	Przechowywanie	Uwagi
Informacja o licencji (email kontaktowy)	Trwałe	Email kontaktowy do obsługi komunikacji związanej z zakupem licencji. Przechowywane trwałe. w przypadku zakupu przez sklep Microsoft email osoby technicznie dokonującej zakupu.
Identyfikatory użytkowników pochodzące z Entra Id	Trwałe	Atrybuty wskazujące użytkowników w różnych encjach danych.
Tokeny dostępowe	Czasowe	Tokeny dostępowe użytkowników wykorzystywane w operacjach długotrwałych przechowywane w Azure Key Vault na czas wykonywania operacji.

Przetwarzanie danych w pamięci podręcznej i operacyjnej

Informacje o użytkownikach prezentowane w interfejsie użytkownika lub wykorzystywane w funkcjonalnościach usługi są pobierane na podstawie zapisywanych trwałe identyfikatorów użytkowników Entra ID.



Podstawowe informacje osobowe uzyskane na podstawie identyfikatorów użytkowników takie jak nazwa wyświetlana, imię, nazwisko, login, adres e-mail mogą czasowo istnieć w pamięci podręcznej przeglądarek użytkowników korzystających z usługi oraz w pamięci operacyjnej po stronie serwera hostującego usługę.

Treści wprowadzane przez użytkowników

Usługa przechowuje dane wprowadzane przez użytkowników lub odnoszące się do środowiska klienta, które mogą zawierać merytoryczne informacje w tym nieustrukturyzowane dane osobowe.

Rodzaj informacji	Przechowywanie	Uwagi
Tytuł i opis w zgłoszeniach użytkowników	Trwałe	Dane przechowywane w Azure SQL, Azure Storage Account (Table).
Treść powiadomień o artykułach (powiadomienie Teams)	Trwałe	Dane przechowywane w Azure SQL, Azure Storage Account (Table).
Adresy witryn SharePoint	Trwałe	Dane przechowywane w Azure SQL, Azure Storage Account (Table).
	Czasowe	Informacje o adresach witryn SharePoint mogą być zapisywane w logach usługi Azure Application Insights.
Informacje o strukturach witryn SharePoint: • nazwy witryn, • tytuły i adresy stron, • nazwy list / bibliotek dokumentów, • nazwy grup.	Trwałe	Adresy stron mogą być zapisywane w Azure SQL, Azure Storage Account (Table) w ramach funkcjonalności raportów Score Cards sprawdzających zgodność witryn SharePoint z zalecaniami i dobrymi praktykami oraz w ramach funkcjonalności powiadomień o artykułach.
Przekazane pliki	Trwałe	Pliki graficzne używane do wygenerowania motywów graficznych przez klientów usługi.
	Czasowe	Pliki informacji źródłowych przekazane przez klientów w procesie generowania portalu. Przechowywane czasowo do momentu utworzenia portalu lub usunięcia projektu portalu.