Google Workspace Data Access Terms - Gmail Inbound And Google Drive

Warunki dostępu do danych Gmail tylko do odczytu

Te warunki wyjaśniają dostęp do Gmaila, o który prosi DynamicMail, gdy upoważniony użytkownik lub administrator tenanta podłącza przyjmowanie dokumentów z Gmaila.

Zakresy tożsamości Google Sign-In, takie jak `openid`, `email` i `profile`, są oddzielne od tej zgody na dostęp do danych Gmaila. Zalogowanie się przez Google nie oznacza akceptacji dostępu do przyjmowania dokumentów z Gmaila.

Żądany zakres

DynamicMail prosi o `https://www.googleapis.com/auth/gmail.readonly` tylko wtedy, gdy upoważniony użytkownik lub administrator tenanta podłącza przyjmowanie dokumentów z Gmaila. Ten ograniczony zakres Gmaila pozwala DynamicMail wyświetlać wiadomości i ustawienia połączonego konta Gmail.

DynamicMail używa tego zakresu do przetwarzania tylko do odczytu. DynamicMail nie używa go do wysyłania, modyfikowania, usuwania, archiwizowania, oznaczania etykietami ani przenoszenia wiadomości Gmail.

DynamicMail nie powinien żądać ani przetwarzać danych Gmaila, które nie są związane z widoczną funkcją przyjmowania dokumentów z Gmaila.

Dane, do których DynamicMail może mieć dostęp

Gdy przyjmowanie dokumentów z Gmaila jest podłączone, DynamicMail może mieć dostęp do danych Gmaila potrzebnych do wyszukiwania i przetwarzania przychodzących dokumentów biznesowych, w tym do:

- identyfikatorów wiadomości, identyfikatorów wątków, identyfikatorów historii, odwołań do etykiet i kursorów synchronizacji;
- nadawcy, odbiorcy, tematu, daty, nagłówków i innych metadanych wiadomości;
- treści wiadomości i fragmentów potrzebnych do rozpoznania kontekstu dokumentu;
- załączników i plików osadzonych, które mogą zawierać faktury, powiadomienia, umowy, potwierdzenia lub inne dokumenty tenanta;
- ustawień Gmaila tylko wtedy, gdy Gmail API wymaga ich dla zakresu tylko do odczytu lub dla działania synchronizacji konta;
- danych pochodnych utworzonych z treści Gmaila, takich jak tekst OCR, sparsowane pola dokumentów, etykiety klasyfikacji, wyniki ekstrakcji, podsumowania, zdarzenia audytowe i rekordy dokumentów.

Cel użycia

DynamicMail używa danych Gmaila tylko do odczytu, aby udostępnić źródło przyjmowania z Gmaila wybrane przez tenanta. Zamierzone cele obejmują:

- wykrywanie przychodzących wiadomości, które mogą zawierać dokumenty biznesowe tenanta;
- importowanie załączników lub treści wiadomości, które tenant wybiera do przetwarzania;
- wyodrębnianie, klasyfikowanie i kierowanie dokumentów do przepływów pracy DynamicMail;
- uzgadnianie stanu synchronizacji, aby ta sama wiadomość nie była importowana wielokrotnie;
- pokazywanie upoważnionym użytkownikom tenanta stanu połączenia, synchronizacji i przetwarzania;
- rozwiązywanie problemów oraz działania związane z bezpieczeństwem, audytem i zgodnością prawną dozwolone przez obowiązujące zasady i umowę z tenantem.

DynamicMail nie może sprzedawać danych Gmaila, używać ich do reklam lub retargetingu, przekazywać ich brokerom danych, używać ich do nadzoru ani używać ich do ustalania zdolności kredytowej lub kwalifikowalności do pożyczki.

Przechowywanie

DynamicMail przechowuje dane pochodzące z Gmaila tylko tak długo, jak jest to potrzebne dla widocznej funkcji przyjmowania dokumentów, ustawień przechowywania dokumentów tenanta, zapisów audytowych, bezpieczeństwa, obsługi sporów lub zgodności prawnej. Tokeny OAuth i metadane synchronizacji są przechowywane tylko tak długo, jak są potrzebne do działania podłączonego źródła przyjmowania z Gmaila lub do zachowania wymaganych zapisów audytowych.

Surowa treść wiadomości Gmail, załączniki i pochodne dane dokumentów powinny zostać usunięte lub zanonimizowane, gdy nie są już potrzebne do ujawnionego celu, chyba że obowiązek prawny, bezpieczeństwa, audytu lub przechowywania określony przez tenanta wymaga dalszego przechowywania.

Usuwanie

Upoważniony użytkownik lub administrator tenanta może zażądać usunięcia buforowanych danych pochodzących z Google, zaimportowanych załączników, wyodrębnionego tekstu i pochodnych rekordów dokumentów. DynamicMail powinien usunąć lub zanonimizować żądane dane, gdy pozwalają na to ustawienia przechowywania tenanta i obowiązujące prawo.

Usunięcie zaimportowanych rekordów DynamicMail nie musi usuwać oryginalnej wiadomości e-mail ani załącznika z Gmaila, ponieważ zakres Gmail tylko do odczytu nie

daje DynamicMail uprawnienia do modyfikowania ani usuwania wiadomości Gmail.

Cofnięcie zgody i odłączenie

Tenant może odłączyć przyjmowanie dokumentów z Gmaila w DynamicMail. Po odłączeniu lub lokalnym cofnięciu zgody DynamicMail musi przestać używać przechowywanych tokenów OAuth dla przyjmowania z Gmaila i musi przestać czytać dodatkowe wiadomości Gmail z połączonego konta.

Właściciel konta Google może także cofnąć autoryzację aplikacji w ustawieniach konta Google. Jeśli autoryzacja Google zostanie cofnięta, DynamicMail musi zatrzymać dostęp do Gmail API, gdy odświeżenie tokenu lub wywołania API się nie powiodą, a połączenie powinno być pokazane jako odłączone lub wymagające ponownego połączenia.

Lokalne cofnięcie zgody nie usuwa automatycznie już zaimportowanych dokumentów DynamicMail. Te rekordy są obsługiwane zgodnie z powyższymi zasadami usuwania i przechowywania.

AI, OCR i ekstrakcja

DynamicMail może używać OCR, parsowania, klasyfikacji, podsumowywania i innego przetwarzania wspomaganego przez AI na treści wiadomości i załącznikach pochodzących z Gmaila tylko w celu udostępnienia lub ulepszenia widocznego przepływu pracy przyjmowania dokumentów dla tenanta. Dane Gmaila i dane pochodne nie mogą być używane do tworzenia, trenowania ani ulepszania ogólnego modelu uczenia maszynowego lub AI poza funkcją zamówioną przez tenanta.

Wyniki wspomagane przez AI mogą być błędne. DynamicMail powinien prezentować wyodrębnione dane jako wynik przepływu pracy, który upoważnieni użytkownicy mogą sprawdzać, poprawiać, zatwierdzać, odrzucać lub usuwać zgodnie z przepływem produktu.

Wsparcie i dostęp człowieka

Personel, wykonawcy lub podprocesorzy DynamicMail nie powinni czytać konkretnych wiadomości Gmail, załączników, wyodrębnionego tekstu ani pochodnych danych Gmaila, chyba że zachodzi jeden z poniższych warunków:

- użytkownik wyraźnie poprosił o wsparcie wymagające dostępu do konkretnych danych;
- dostęp jest niezbędny do dochodzenia bezpieczeństwa, zapobiegania nadużyciom lub reagowania na incydent;
- dostęp jest niezbędny do przestrzegania prawa, procesu prawnego lub wiążącej instrukcji tenanta;
- dane są zagregowane lub zanonimizowane na potrzeby wewnętrznych operacji, a treść Gmaila konkretnego użytkownika nie jest możliwa do odczytania.

Dostęp wsparcia powinien być oparty na zasadzie najmniejszych uprawnień, w praktycznym zakresie ograniczony czasowo i rejestrowany na potrzeby audytu.

Jest to lokalizowany materiał wdrożeniowy i przeglądowy, a nie ostateczna porada prawna ani lokalna porada prawna. Bez osobnego dowodu oceny nie wolno przedstawiać go jako mającego poparcie Google, akceptację zewnętrznego doradcy prawnego lub produkcyjne dopuszczenie restricted-scope.

Referencje

- DynamicMail restricted-scope contract: `Documentation/DynamicMail/LocalizedIntegrations/google-restricted-scope-compliance-contract-2026-06-02.md`
- Google API Services User Data Policy: https://developers.google.com/terms/api-services-user-data-policy
- Google Workspace API user data and developer policy: https://developers.google.com/workspace/workspace-api-user-data-developer-policy
- Gmail API scopes: https://developers.google.com/workspace/gmail/api/auth/scopes
- Google restricted-scope verification guidance: https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification

Warunki dostępu do danych Google Drive

Te warunki wyjaśniają dostęp do Google Drive, o który prosi DynamicMail, gdy upoważniony użytkownik lub administrator tenanta podłącza Google Drive do przepływów pracy z dokumentami tenanta.

Zakresy tożsamości Google Sign-In, takie jak `openid`, `email` i `profile`, są oddzielne od tej zgody na dostęp do danych Google Drive. Zalogowanie się przez Google nie oznacza akceptacji dostępu do Google Drive.

Żądany zakres

DynamicMail prosi o `https://www.googleapis.com/auth/drive` tylko wtedy, gdy upoważniony użytkownik lub administrator tenanta podłącza Google Drive do przepływów pracy z dokumentami tenanta. Jest to szeroki ograniczony zakres Drive, który może pozwalać DynamicMail wyświetlać i zarządzać wszystkimi plikami na połączonym koncie Google Drive, w tym plikami należącymi do użytkownika, plikami udostępnionymi użytkownikowi, folderami oraz treścią dysków współdzielonych dostępną dla tego konta.

DynamicMail musi używać zakresu Drive tylko do ujawnionych, widocznych przepływów pracy z dokumentami Drive wybranych przez tenanta. DynamicMail nie powinien żądać, przeglądać, kopiować, pobierać, modyfikować, usuwać ani w inny sposób przetwarzać danych Drive, które nie są związane z widocznym przepływem pracy z dokumentami Drive.

Dane, do których DynamicMail może mieć dostęp

Gdy Google Drive jest podłączony, DynamicMail może mieć dostęp do danych Drive potrzebnych do udostępnienia wybranego przepływu pracy tenanta, w tym do:

- identyfikatorów plików, nazw, typów MIME, sum kontrolnych, rozmiaru, znaczników czasu, opisów, etykiet, odwołań do folderów, folderów nadrzędnych i innych metadanych plików;
- metadanych folderów, metadanych dysków współdzielonych oraz wyników wyszukiwania lub listowania potrzebnych do znalezienia dokumentów tenanta;
- treści plików, podglądów, miniatur, eksportów, pobrań, przesłań oraz wygenerowanych lub edytowanych ładunków plików;
- metadanych udostępniania i uprawnień, gdy są potrzebne do pokazania lub ukończenia widocznej operacji na pliku Drive;
- podsumowania informacji Drive na poziomie konta, potrzebnego do potwierdzenia połączonego konta i stanu połączenia;
- przechowywanych kopii lub buforowanych wyciągów z plików Drive zaimportowanych do DynamicMail;
- danych pochodnych utworzonych z plików Drive, takich jak tekst OCR, sparsowane pola dokumentów, etykiety klasyfikacji, wyniki ekstrakcji, podsumowania, zdarzenia audytowe i rekordy dokumentów.

Cel użycia

DynamicMail używa danych Google Drive, aby udostępniać przepływy pracy z dokumentami Drive wybrane przez tenanta. Zamierzone cele obejmują:

- umożliwianie upoważnionym użytkownikom podłączenia Drive jako źródła dokumentów lub miejsca docelowego;
- znajdowanie, listowanie, importowanie, pobieranie, eksportowanie, przesyłanie lub aktualizowanie dokumentów biznesowych tenanta wybranych w przepływie produktu;
- wyodrębnianie, klasyfikowanie i kierowanie dokumentów Drive do przepływów pracy DynamicMail;
- pokazywanie upoważnionym użytkownikom tenanta stanu połączenia, operacji na plikach, synchronizacji i przetwarzania;
- utrzymywanie zapisów audytowych i dzienników operacyjnych, które potwierdzają, jaka operacja Drive została zażądana i wykonana;
- rozwiązywanie problemów oraz działania związane z bezpieczeństwem, zapobieganiem nadużyciom, obsługą sporów i zgodnością prawną dozwolone przez obowiązujące zasady i umowę z tenantem.

DynamicMail nie może sprzedawać danych Google Drive, używać ich do reklam lub retargetingu, przekazywać ich brokerom danych, używać ich do nadzoru ani używać ich

do ustalania zdolności kredytowej lub kwalifikowalności do pożyczki.

Szeroki zakres Drive i uwaga o najwęższym zakresie

Zakres `https://www.googleapis.com/auth/drive` jest szeroki, ponieważ może pozwalać na dostęp do wszystkich plików Drive dostępnych dla połączonego konta. DynamicMail musi traktować ten zakres jako tymczasowy, dopóki przegląd produktu i zgodności nie udokumentuje, dlaczego węższe zakresy Drive są niewystarczające dla wdrożonego przepływu pracy.

Przed użyciem produkcyjnym DynamicMail powinien ocenić węższe zakresy Drive, takie jak `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` lub `drive.appfolder`. Jeśli węższy zakres może obsłużyć widoczną funkcję, żądany zakres, rekordy zgody, konfiguracja OAuth, zasób źródłowy, wygenerowany zasób i testy muszą zostać zaktualizowane przed wydaniem.

Przechowywanie

DynamicMail przechowuje dane pochodzące z Drive tylko tak długo, jak jest to potrzebne dla widocznego przepływu pracy Drive, ustawień przechowywania dokumentów tenanta, zapisów audytowych, bezpieczeństwa, obsługi sporów lub zgodności prawnej. Tokeny OAuth i metadane operacji Drive są przechowywane tylko tak długo, jak są potrzebne do działania podłączonej integracji Drive lub do zachowania wymaganych zapisów audytowych.

Treść plików Drive, buforowane pliki, metadane, tekst OCR, wyodrębnione pola i pochodne dane dokumentów powinny zostać usunięte lub zanonimizowane, gdy nie są już potrzebne do ujawnionego celu, chyba że obowiązek prawny, bezpieczeństwa, audytu lub przechowywania określony przez tenanta wymaga dalszego przechowywania.

Usuwanie

Upoważniony użytkownik lub administrator tenanta może zażądać usunięcia buforowanych danych pochodzących z Google, zaimportowanych plików Drive, wyodrębnionego tekstu i pochodnych rekordów dokumentów. DynamicMail powinien usunąć lub zanonimizować żądane dane, gdy pozwalają na to ustawienia przechowywania tenanta i obowiązujące prawo.

Usunięcie zaimportowanych rekordów DynamicMail nie musi usuwać oryginalnego pliku z Google Drive. DynamicMail powinien modyfikować, przenosić, przenosić do kosza lub usuwać oryginalne pliki Drive tylko wtedy, gdy upoważniony użytkownik wyraźnie zażąda takiego działania Drive przez widoczny przepływ produktu, a działanie jest dozwolone przez politykę tenanta i obowiązujące prawo.

Cofnięcie zgody i odłączenie

Tenant może odłączyć Google Drive w DynamicMail. Po odłączeniu lub lokalnym cofnięciu zgody DynamicMail musi przestać używać przechowywanych tokenów OAuth dla Google

Drive i musi przestać czytać, zapisywać, pobierać, przesyłać, modyfikować lub usuwać dodatkowe pliki Drive z połączonego konta.

Właściciel konta Google może także cofnąć autoryzację aplikacji w ustawieniach konta Google. Jeśli autoryzacja Google zostanie cofnięta, DynamicMail musi zatrzymać dostęp do Drive API, gdy odświeżenie tokenu lub wywołania API się nie powiodą, a połączenie powinno być pokazane jako odłączone lub wymagające ponownego połączenia.

Lokalne cofnięcie zgody nie usuwa automatycznie już zaimportowanych dokumentów DynamicMail. Te rekordy są obsługiwane zgodnie z powyższymi zasadami usuwania i przechowywania.

AI, OCR i ekstrakcja

DynamicMail może używać OCR, parsowania, klasyfikacji, podsumowywania i innego przetwarzania wspomaganego przez AI na treści plików i metadanych Drive tylko w celu udostępnienia lub ulepszenia widocznego przepływu pracy z dokumentami Drive dla tenanta. Dane Drive i dane pochodne nie mogą być używane do tworzenia, trenowania ani ulepszania ogólnego modelu uczenia maszynowego lub AI poza funkcją zamówioną przez tenanta.

Wyniki wspomagane przez AI mogą być błędne. DynamicMail powinien prezentować wyodrębnione dane jako wynik przepływu pracy, który upoważnieni użytkownicy mogą sprawdzać, poprawiać, zatwierdzać, odrzucać lub usuwać zgodnie z przepływem produktu.

Wsparcie i dostęp człowieka

Personel, wykonawcy lub podprocesorzy DynamicMail nie powinni czytać konkretnych plików Drive, wyodrębnionego tekstu, metadanych plików ani pochodnych danych Drive, chyba że zachodzi jeden z poniższych warunków:

- użytkownik wyraźnie poprosił o wsparcie wymagające dostępu do konkretnych danych;
- dostęp jest niezbędny do dochodzenia bezpieczeństwa, zapobiegania nadużyciom lub reagowania na incydent;
- dostęp jest niezbędny do przestrzegania prawa, procesu prawnego lub wiążącej instrukcji tenanta;
- dane są zagregowane lub zanonimizowane na potrzeby wewnętrznych operacji, a treść Drive konkretnego użytkownika nie jest możliwa do odczytania.

Dostęp wsparcia powinien być oparty na zasadzie najmniejszych uprawnień, w praktycznym zakresie ograniczony czasowo i rejestrowany na potrzeby audytu.

Jest to lokalizowany materiał wdrożeniowy i przeglądowy, a nie ostateczna porada prawna ani lokalna porada prawna. Bez osobnego dowodu oceny nie wolno przedstawiać

go jako mającego poparcie Google, akceptację zewnętrznego doradcy prawnego lub produkcyjne dopuszczenie restricted-scope.

Referencje

- DynamicMail Restricted-Scope Contract: `Documentation/DynamicMail/LocalizedIntegrations/google-restricted-scope-compliance-contract-2026-06-02.md`
- Google API Services User Data Policy: https://developers.google.com/terms/api-services-user-data-policy
- Google Workspace API user data and developer policy: https://developers.google.com/workspace/workspace-api-user-data-developer-policy
- Google Drive API scopes: https://developers.google.com/workspace/drive/api/guides/api-specific-auth
- Google restricted-scope verification guidance: https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification