

Conditions d'accès aux données Google Drive

Ces conditions expliquent l'accès Google Drive que DynamicMail demande lorsqu'un utilisateur ou administrateur autorise de l'organisation cliente connecte Google Drive pour les flux de documents de l'organisation cliente.

Ce document couvre uniquement Google Drive. Il est destiné à être utilisé avec les conditions Gmail en lecture seule de la même famille d'actifs Google Workspace.

Portée

DynamicMail demande <https://www.googleapis.com/auth/drive> uniquement lorsqu'un utilisateur ou administrateur autorise de l'organisation cliente connecte Google Drive pour les flux de documents de l'organisation cliente. Il s'agit d'une portée Drive restreinte large qui peut permettre à DynamicMail de consulter et gérer tous les fichiers du compte Google Drive connecté, y compris les fichiers dont l'utilisateur est propriétaire, les fichiers partagés avec l'utilisateur, les dossiers et le contenu des drives partagés accessibles à ce compte.

DynamicMail doit utiliser la portée Drive uniquement pour les flux de documents Drive visibles et déclarés qui sont sélectionnés par l'organisation cliente. Les portées d'identité Google Sign-In telles que `openid`, `email` et `profile` sont séparées de ce consentement d'accès aux données Drive. Se connecter avec Google ne vaut pas acceptation de l'accès Google Drive.

Données auxquelles DynamicMail peut accéder

Lorsque Google Drive est connecté, DynamicMail peut accéder aux données Drive nécessaires pour fournir le flux de travail choisi par l'organisation cliente, notamment:

- les identifiants de fichiers, noms, types MIME, sommes de contrôle, tailles, horodatages, descriptions, libelles, références de dossiers, dossiers parents et autres métadonnées de fichier;
- les métadonnées de dossiers, les métadonnées de drives partagés et les résultats de recherche ou de listage nécessaires pour localiser les documents de l'organisation cliente;
- le contenu de fichiers, les aperçus, miniatures, exports, téléchargements, chargements et charges utiles de fichiers générées ou modifiées;
- les métadonnées de partage et d'autorisations lorsqu'elles sont nécessaires pour afficher ou effectuer une opération Drive visible sur un fichier;

- les informations de synthèse au niveau du compte Drive nécessaires pour confirmer le compte connecté et l'état de connexion;
- les copies stockées ou extraits mis en cache de fichiers Drive importés dans DynamicMail;
- les données dérivées créées à partir de fichiers Drive, comme le texte OCR, les champs de document analysés, les libelles de classification, les résultats d'extraction, les résumés, les événements d'audit et les enregistrements de documents.

DynamicMail ne devrait pas demander, parcourir, copier, télécharger, modifier, supprimer ni traiter autrement des données Drive sans rapport avec le flux de documents Drive visible.

Finalité

DynamicMail utilise les données Google Drive pour fournir les flux de documents Drive sélectionnés par l'organisation cliente. Les finalités prévues sont:

- permettre aux utilisateurs autorisés de connecter Drive comme source ou destination de documents;
- trouver, lister, importer, télécharger, exporter, charger ou mettre à jour les documents professionnels de l'organisation cliente sélectionnés dans le parcours produit;
- extraire, classer et acheminer les documents Drive dans les flux de travail DynamicMail;
- afficher l'état de connexion, d'opération sur fichier, de synchronisation et de traitement aux utilisateurs autorisés de l'organisation cliente;
- maintenir des enregistrements d'audit et des journaux opérationnels prouvant quelle opération Drive a été demandée et terminée;
- effectuer les activités de dépannage, de sécurité, de prévention des abus, de traitement des litiges et de conformité juridique autorisées par les politiques applicables et l'accord avec l'organisation cliente.

DynamicMail ne doit pas vendre les données Google Drive, les utiliser pour la publicité ou le ciblage, les transférer à des courtiers en données, les utiliser à des fins de surveillance, ni les utiliser pour déterminer la solvabilité ou l'éligibilité à un prêt.

Note sur la portée large et la portée la plus restrictive

La portée <https://www.googleapis.com/auth/drive> est large, car elle peut permettre l'accès à tous les fichiers Drive disponibles pour le compte connecté. DynamicMail doit traiter cette portée comme provisoire jusqu'à ce que la revue produit et conformité documente pourquoi des portées Drive plus étroites sont insuffisantes pour le flux de travail implémenté.

Avant une utilisation en production, DynamicMail devrait evaluer des portees Drive plus etroites telles que `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` ou `drive.appfolder`. Si une portee plus etroite peut prendre en charge la fonctionnalite visible, la portee demandee, les enregistrements de consentement, la configuration OAuth, l'actif source, l'actif rendu et les tests doivent etre mis a jour avant la publication.

Conservation

DynamicMail conserve les donnees derivees de Drive uniquement aussi longtemps que necessaire pour le flux Drive visible, les parametres de conservation des documents de l'organisation cliente, les enregistrements d'audit, la securite, le traitement des litiges ou la conformite juridique. Les jetons OAuth et les metadonnees d'operation Drive sont conservees uniquement pendant la duree necessaire pour exploiter l'integration Drive connectee ou conserver les enregistrements d'audit requis.

Le contenu des fichiers Drive, les fichiers mis en cache, les metadonnees, le texte OCR, les champs extraits et les donnees de document derivees devraient etre supprimees ou anonymisees lorsqu'ils ne sont plus necessaires a la finalite declaree, sauf si une obligation juridique, de securite, d'audit ou de conservation de l'organisation cliente exige leur conservation continue.

Suppression

Un utilisateur ou administrateur autorise de l'organisation cliente peut demander la suppression des donnees Google mises en cache, des fichiers Drive importes, du texte extrait et des enregistrements de documents derives. DynamicMail devrait supprimer ou anonymiser les donnees demandees lorsque les parametres de conservation de l'organisation cliente et le droit applicable le permettent.

La suppression des enregistrements importes dans DynamicMail ne supprime pas necessairement le fichier d'origine dans Google Drive. DynamicMail devrait modifier, deplacer, placer dans la corbeille ou supprimer les fichiers Drive d'origine uniquement lorsqu'un utilisateur autorise demande explicitement cette action Drive dans un flux produit visible et lorsque l'action est autorisee par la politique de l'organisation cliente et le droit applicable.

Revocation et deconnexion

L'organisation cliente peut deconnecter Google Drive dans DynamicMail. Apres une deconnexion ou une revocation locale du consentement, DynamicMail doit cesser d'utiliser les jetons OAuth stockes pour Google Drive et doit cesser de lire, ecrire, telecharger, charger, modifier ou supprimer d'autres fichiers Drive depuis le compte connecte.

Le proprietaire du compte Google peut egalement revoquer l'autorisation de l'application dans les parametres du compte Google. Si l'autorisation Google est revoquee,

DynamicMail doit cesser l'accès à l'API Drive lorsque l'actualisation des jetons ou les appels API échouent, et la connexion devrait être affichée comme déconnectée ou nécessitant une reconnexion.

La révocation locale ne supprime pas automatiquement les documents DynamicMail déjà importés. Ces enregistrements sont traités selon les règles de suppression et de conservation ci-dessus.

Utilisation de l'IA, de l'OCR et de l'extraction

DynamicMail peut utiliser l'OCR, l'analyse, la classification, le résumé et d'autres traitements assistés par l'IA sur le contenu et les métadonnées de fichiers Drive uniquement pour fournir ou améliorer le flux de documents Drive visible de l'organisation cliente. Les données Drive et les données dérivées ne doivent pas être utilisées pour créer, entraîner ou améliorer un modèle d'apprentissage automatique ou d'IA à usage général en dehors de la fonctionnalité demandée par l'organisation cliente.

Les résultats assistés par l'IA peuvent être incorrects. DynamicMail devrait présenter les données extraites comme une sortie de flux de travail que les utilisateurs autorisés peuvent examiner, corriger, approuver, rejeter ou supprimer selon le parcours produit.

Accès par le support et par des personnes

Le personnel, les contractants ou les sous-traitants de DynamicMail ne devraient pas lire des fichiers Drive, textes extraits, métadonnées de fichier ou données Drive dérivées spécifiques, sauf si l'une des conditions suivantes s'applique:

- l'utilisateur a explicitement demandé une assistance qui nécessite l'accès à des données spécifiques;
- l'accès est nécessaire pour une enquête de sécurité, la prévention des abus ou la réponse à un incident;
- l'accès est nécessaire pour se conformer à la loi, à une procédure juridique ou à une instruction contraignante de l'organisation cliente;
- les données sont agrégées ou anonymisées pour les opérations internes et aucun contenu Drive d'un utilisateur spécifique n'est lisible.

L'accès par le support devrait être fondé sur le moindre privilège, limité dans le temps lorsque cela est pratique, et journalisé à des fins d'audit.

Il s'agit d'un support d'implémentation et de localisation, pas d'un avis juridique final. Il ne doit pas être présenté comme portant une approbation de Google, une validation par un conseil externe ou une autorisation de production pour portée restreinte sans preuve de revue distincte.

References sources

- 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>