DYNAMICMAIL GOOGLE WORKSPACE TERMS

Conditions d'acces aux donnees Google Drive

Ces conditions expliquent l'acces 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 destine a etre utilise avec les conditions Gmail en lecture seule de la meme famille d'actifs Google Workspace.

Portee

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 portee Drive restreinte large qui peut permettre a DynamicMail de consulter et gerer tous les fichiers du compte Google Drive connecte, y compris les fichiers dont l'utilisateur est proprietaire, les fichiers partages avec l'utilisateur, les dossiers et le contenu des drives partages accessibles a ce compte.

DynamicMail doit utiliser la portee Drive uniquement pour les flux de documents Drive visibles et declares qui sont selectionnes par l'organisation cliente. Les portees d'identite Google Sign-In telles que `openid`, `email` et `profile` sont separees de ce consentement d'acces aux donnees Drive. Se connecter avec Google ne vaut pas acceptation de l'acces Google Drive.

Donnees auxquelles DynamicMail peut acceder

Lorsque Google Drive est connecte, DynamicMail peut acceder aux donnees Drive necessaires pour fournir le flux de travail choisi par l'organisation cliente, notamment:

- les identifiants de fichiers, noms, types MIME, sommes de controle, tailles, horodatages, descriptions, libelles, references de dossiers, dossiers parents et autres metadonnees de fichier;
- les metadonnees de dossiers, les metadonnees de drives partages et les resultats de recherche ou de listage necessaires pour localiser les documents de l'organisation cliente;
- le contenu de fichiers, les apercus, miniatures, exports, telechargements, chargements et charges utiles de fichiers generees ou modifiees;
- les metadonnees de partage et d'autorisations lorsqu'elles sont necessaires pour afficher ou effectuer une operation Drive visible sur un fichier;

- les informations de synthese au niveau du compte Drive necessaires pour confirmer le compte connecte et l'etat de connexion;
- les copies stockees ou extraits mis en cache de fichiers Drive importes dans DynamicMail;
- les donnees derivees creees a partir de fichiers Drive, comme le texte OCR, les champs de document analyses, les libelles de classification, les resultats d'extraction, les resumes, les evenements d'audit et les enregistrements de documents.

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

Finalite

DynamicMail utilise les donnees Google Drive pour fournir les flux de documents Drive selectionnes par l'organisation cliente. Les finalites prevues sont:

- permettre aux utilisateurs autorises de connecter Drive comme source ou destination de documents;
- trouver, lister, importer, telecharger, exporter, charger ou mettre a jour les documents professionnels de l'organisation cliente selectionnes dans le parcours produit;
- extraire, classer et acheminer les documents Drive dans les flux de travail DynamicMail;
- afficher l'etat de connexion, d'operation sur fichier, de synchronisation et de traitement aux utilisateurs autorises de l'organisation cliente;
- maintenir des enregistrements d'audit et des journaux operationnels prouvant quelle operation Drive a ete demandee et terminee;
- effectuer les activites de depannage, de securite, de prevention des abus, de traitement des litiges et de conformite juridique autorisees par les politiques applicables et l'accord avec l'organisation cliente.

DynamicMail ne doit pas vendre les donnees Google Drive, les utiliser pour la publicite ou le reciblage, les transferer a des courtiers en donnees, les utiliser a des fins de surveillance, ni les utiliser pour determiner la solvabilite ou l'eligibilite a un pret.

Note sur la portee large et la portee la plus restrictive

La portee `https://www.googleapis.com/auth/drive` est large, car elle peut permettre l'acces a tous les fichiers Drive disponibles pour le compte connecte. DynamicMail doit traiter cette portee comme provisoire jusqu'a ce que la revue produit et conformite documente pourquoi des portees Drive plus etroites sont insuffisantes pour le flux de travail implemente.

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 conserves 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 supprimes ou anonymises 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'acces a l'API Drive lorsque l'actualisation des jetons ou les appels API echouent, et la connexion devrait etre affichee comme deconnectee ou necessitant une reconnexion.

La revocation locale ne supprime pas automatiquement les documents DynamicMail deja importes. Ces enregistrements sont traites selon les regles 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 resume et d'autres traitements assistes par l'IA sur le contenu et les metadonnees de fichiers Drive uniquement pour fournir ou ameliorer le flux de documents Drive visible de l'organisation cliente. Les donnees Drive et les donnees derivees ne doivent pas etre utilisees pour creer, entrainer ou ameliorer un modele d'apprentissage automatique ou d'IA a usage general en dehors de la fonctionnalite demandee par l'organisation cliente.

Les resultats assistes par l'IA peuvent etre incorrects. DynamicMail devrait presenter les donnees extraites comme une sortie de flux de travail que les utilisateurs autorises peuvent examiner, corriger, approuver, rejeter ou supprimer selon le parcours produit.

Acces 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, metadonnees de fichier ou donnees Drive derivees specifiques, sauf si l'une des conditions suivantes s'applique:

- l'utilisateur a explicitement demande une assistance qui necessite l'acces a des donnees specifiques;
- l'acces est necessaire pour une enquete de securite, la prevention des abus ou la reponse a un incident;
- l'acces est necessaire pour se conformer a la loi, a une procedure juridique ou a une instruction contraignante de l'organisation cliente;
- les donnees sont agregees ou anonymisees pour les operations internes et aucun contenu Drive d'un utilisateur specifique n'est lisible.

L'acces par le support devrait etre fonde sur le moindre privilege, limite dans le temps lorsque cela est pratique, et journalise a des fins d'audit.

Il s'agit d'un support d'implementation et de localisation, pas d'un avis juridique final. Il ne doit pas etre presente comme portant une approbation de Google, une validation par un conseil externe ou une autorisation de production pour portee 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