

Termos de acesso a dados do Google Drive

Estes termos explicam o acesso restrito ao Google Drive que a DynamicMail solicita para <https://www.googleapis.com/auth/drive> quando um usuário autorizado ou administrador do cliente conecta o Google Drive para fluxos de trabalho de documentos.

Este ativo cobre apenas o Google Drive. Ele se destina a ser usado junto com os termos de Gmail somente leitura dentro da família de ativos `google-workspace-data-access`.

Escopo

A DynamicMail solicita <https://www.googleapis.com/auth/drive> somente quando um usuário autorizado ou administrador do cliente conecta o Google Drive para fluxos de trabalho de documentos do cliente. Este é um escopo restrito amplo do Drive que pode permitir que a DynamicMail visualize e gerencie todos os arquivos na conta Google Drive conectada, incluindo arquivos pertencentes ao usuário, arquivos compartilhados com o usuário, pastas e conteúdo de drives compartilhados disponível para essa conta.

A DynamicMail deve usar o escopo do Drive somente para fluxos de trabalho visíveis de documentos do Drive, informados e selecionados pelo cliente. Os escopos de identidade do Google Sign-In, como `openid`, `email` e `profile`, são separados deste consentimento de acesso a dados do Drive. Entrar com o Google não significa aceitar o acesso ao Google Drive.

Dados que a DynamicMail pode acessar

Quando o Google Drive está conectado, a DynamicMail pode acessar os dados do Drive necessários para fornecer o fluxo selecionado pelo cliente, incluindo:

- IDs de arquivos, nomes, tipos MIME, checksums, tamanho, carimbos de data e hora, descrições, rótulos, referências de pastas, pastas principais e outros metadados de arquivos;
- metadados de pastas, metadados de drives compartilhados e resultados de pesquisa/listagem necessários para localizar documentos do cliente;
- conteúdo de arquivos, pré-visualizações, miniaturas, exportações, downloads, uploads e payloads de arquivos gerados ou editados;
- metadados de compartilhamento e permissões quando necessários para exibir ou concluir uma operação visível em arquivos do Drive;
- informações resumidas em nível de conta do Drive necessárias para confirmar a conta conectada e o status da conexão;

- cópias armazenadas ou extratos em cache de arquivos do Drive importados para a DynamicMail;
- dados derivados criados a partir de arquivos do Drive, como texto de OCR, campos de documentos processados, rótulos de classificação, resultados de extração, resumos, eventos de auditoria e registros de documentos.

A DynamicMail não deve solicitar, navegar, copiar, baixar, modificar, excluir nem processar de outra forma dados do Drive que não estejam relacionados ao fluxo visível de documentos do Drive.

Por que a DynamicMail usa dados do Google Drive

A DynamicMail usa dados do Google Drive para fornecer fluxos de trabalho de documentos do Drive selecionados pelo cliente. As finalidades previstas são:

- permitir que usuários autorizados conectem o Drive como fonte ou destino de documentos;
- localizar, listar, importar, baixar, exportar, enviar ou atualizar documentos comerciais do cliente selecionados por meio do fluxo do produto;
- extrair, classificar e encaminhar documentos do Drive nos fluxos de trabalho da DynamicMail;
- exibir o status de conexão, operações de arquivos, sincronização e processamento para usuários autorizados do cliente;
- manter registros de auditoria e logs operacionais que comprovem qual operação do Drive foi solicitada e concluída;
- realizar atividades de suporte, segurança, prevenção de abuso, tratamento de disputas e conformidade legal permitidas pelas políticas aplicáveis e pelo acordo com o cliente.

A DynamicMail não deve vender dados do Google Drive, usá-los para publicidade ou retargeting, transferi-los a corretores de dados, usá-los para vigilância nem usá-los para determinar capacidade de crédito ou elegibilidade para empréstimos.

Observação sobre escopo amplo e escopo mais restrito

O escopo <https://www.googleapis.com/auth/drive> é amplo porque pode permitir acesso a todos os arquivos do Drive disponíveis para a conta conectada. A DynamicMail deve tratar este escopo como provisório até que a revisão de produto e conformidade documente por que escopos do Drive mais restritos são insuficientes para o fluxo implementado.

Antes do uso em produção, a DynamicMail deve avaliar escopos do Drive mais restritos, como `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` ou `drive.appfolder`. Se um escopo mais restrito puder dar suporte ao recurso visível, o

escopo solicitado, os registros de consentimento, a configuração OAuth, o ativo fonte, o ativo renderizado e os testes devem ser atualizados antes do lançamento.

Retenção

A DynamicMail retém dados derivados do Drive somente pelo tempo necessário para o fluxo visível do Drive, as configurações de retenção de documentos do cliente, registros de auditoria, segurança, tratamento de disputas ou conformidade legal. Tokens OAuth e metadados de operações do Drive são retidos somente enquanto forem necessários para operar a integração do Drive conectada ou para preservar registros de auditoria exigidos.

Conteúdo de arquivos do Drive, arquivos em cache, metadados, texto de OCR, campos extraídos e dados de documentos derivados devem ser excluídos ou anonimizados quando não forem mais necessários para a finalidade informada, salvo se uma obrigação legal, de segurança, de auditoria ou de retenção do cliente exigir retenção contínua.

Exclusão

Um usuário autorizado ou administrador do cliente pode solicitar a exclusão de dados em cache derivados do Google, arquivos do Drive importados, texto extraído e registros de documentos derivados. A DynamicMail deve excluir ou anonimizar os dados solicitados quando isso for permitido pelas configurações de retenção do cliente e pela lei aplicável.

Excluir registros importados da DynamicMail não exclui necessariamente o arquivo original do Google Drive. A DynamicMail deve modificar, mover para a lixeira ou excluir arquivos originais do Drive somente quando um usuário autorizado solicitar explicitamente essa ação do Drive por meio de um fluxo visível do produto e a ação for permitida pela política do cliente e pela lei aplicável.

Revogação e desconexão

O cliente pode desconectar o Google Drive na DynamicMail. Após a desconexão ou a revogação local do consentimento, a DynamicMail deve parar de usar tokens OAuth armazenados para o Google Drive e deve parar de ler, escrever, baixar, enviar, modificar ou excluir arquivos adicionais do Drive da conta conectada.

O proprietário da conta Google também pode revogar a autorização do aplicativo nas configurações da conta Google. Se a autorização do Google for revogada, a DynamicMail deve interromper o acesso à API do Drive quando a renovação do token ou as chamadas à API falharem, e a conexão deve ser exibida como desconectada ou exigindo reconexão.

A revogação local não remove automaticamente documentos já importados para a DynamicMail. Esses registros são tratados pelas regras de exclusão e retenção acima.

Uso de IA, OCR e extração

A DynamicMail pode usar OCR, processamento, classificação, resumos e outros tratamentos assistidos por IA sobre conteúdo e metadados de arquivos derivados do Drive somente para fornecer ou melhorar o fluxo visível de documentos do Drive solicitado pelo cliente. Dados do Drive e dados derivados não devem ser usados para criar, treinar ou melhorar um modelo geral de aprendizado de máquina ou IA fora do recurso solicitado pelo cliente.

Resultados assistidos por IA podem estar incorretos. A DynamicMail deve apresentar os dados extraídos como saída de fluxo de trabalho que usuários autorizados podem revisar, corrigir, aprovar, rejeitar ou excluir de acordo com o fluxo do produto.

Acesso de suporte e acesso humano

Funcionários, contratados ou subprocessadores da DynamicMail não devem ler arquivos específicos do Drive, texto extraído, metadados de arquivos ou dados derivados do Drive, salvo se uma destas condições se aplicar:

- o usuário solicitou explicitamente suporte que exige acesso a dados específicos;
- o acesso é necessário para investigação de segurança, prevenção de abuso ou resposta a incidente;
- o acesso é necessário para cumprir a lei, processo legal ou uma instrução vinculante do cliente;
- os dados estão agregados ou anonimizados para operações internas e nenhum conteúdo do Drive de um usuário específico é legível.

O acesso de suporte deve usar o menor privilégio necessário, ser limitado no tempo quando praticável e ser registrado para fins de auditoria.

Ele é material de implementação e localização, não aconselhamento jurídico final. Ele não deve ser apresentado como tendo endosso do Google, aprovação de assessoria jurídica externa ou autorização de produção para escopos restritos sem evidência separada de revisão.

Referências fonte

- Contrato de escopo restrito da DynamicMail:
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>