

Termos de acesso a dados do Google Drive

Estes termos explicam o acesso ao Google Drive que a DynamicMail solicita quando um utilizador autorizado ou administrador do cliente liga o Google Drive aos fluxos de trabalho de documentos do cliente.

Os âmbitos de identidade do Google Sign-In, como openid, email e profile, são separados deste consentimento de acesso a dados do Google Drive. Iniciar sessão com o Google não significa aceitar o acesso ao Google Drive.

Âmbito solicitado

A DynamicMail solicita <https://www.googleapis.com/auth/drive> apenas quando um utilizador autorizado ou administrador do cliente liga o Google Drive aos fluxos de trabalho de documentos do cliente. Este é um âmbito restrito amplo do Drive que pode permitir à DynamicMail ver e gerir todos os ficheiros na conta Google Drive ligada, incluindo ficheiros pertencentes ao utilizador, ficheiros partilhados com o utilizador, pastas e conteúdo de drives partilhados disponível para essa conta.

A DynamicMail deve utilizar o âmbito do Drive apenas para fluxos de trabalho visíveis de documentos do Drive, comunicados e selecionados pelo cliente. A DynamicMail não deve solicitar, navegar, copiar, transferir, modificar, eliminar ou tratar de outra forma dados do Drive que não estejam relacionados com o fluxo de trabalho visível de documentos do Drive.

Dados aos quais a DynamicMail pode aceder

Quando o Google Drive está ligado, a DynamicMail pode aceder aos dados do Drive necessários para fornecer o fluxo de trabalho selecionado pelo cliente, incluindo:

- IDs de ficheiros, nomes, tipos MIME, checksums, tamanho, carimbos de data/hora, descrições, etiquetas, referências de pastas, pastas principais e outros metadados de ficheiros;
- metadados de pastas, metadados de drives partilhados e resultados de pesquisa ou listagem necessários para localizar documentos do cliente;
- conteúdo de ficheiros, pré-visualizações, miniaturas, exportações, transferências, carregamentos e payloads de ficheiros gerados ou editados;
- metadados de partilha e permissões quando necessários para mostrar ou concluir uma operação visível sobre ficheiros do Drive;

- informação resumida ao nível da conta do Drive necessária para confirmar a conta ligada e o estado da ligação;
- cópias armazenadas ou extratos em cache de ficheiros do Drive importados para a DynamicMail;
- dados derivados criados a partir de ficheiros do Drive, como texto de OCR, campos de documentos analisados, etiquetas de classificação, resultados de extração, resumos, eventos de auditoria e registos de documentos.

Finalidade da utilização

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

- permitir que utilizadores autorizados liguem o Drive como origem ou destino de documentos;
- encontrar, listar, importar, transferir, exportar, carregar ou atualizar documentos comerciais do cliente selecionados através do fluxo do produto;
- extrair, classificar e encaminhar documentos do Drive para fluxos de trabalho da DynamicMail;
- mostrar o estado de ligação, operações sobre ficheiros, sincronização e processamento a utilizadores autorizados do cliente;
- manter registos de auditoria e logs operacionais que comprovem que operação do Drive foi solicitada e concluída;
- resolução de problemas, segurança, prevenção de abuso, gestão de litígios e atividades de conformidade jurídica permitidas pelas políticas aplicáveis e pelo acordo com o cliente.

A DynamicMail não deve vender dados do Google Drive, utilizá-los para publicidade ou retargeting, transferi-los para corretores de dados, utilizá-los para vigilância ou utilizá-los para determinar solvabilidade ou elegibilidade para empréstimos.

Âmbito amplo do Drive e nota de narrowest-scope

O âmbito <https://www.googleapis.com/auth/drive> é amplo porque pode permitir acesso a todos os ficheiros do Drive disponíveis para a conta ligada. A DynamicMail deve tratar este âmbito como provisório até que a revisão de produto e conformidade documente por que motivo âmbitos do Drive mais restritos não são suficientes para o fluxo de trabalho implementado.

Antes da utilização em produção, a DynamicMail deve avaliar âmbitos do Drive mais restritos, como `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` ou `drive.appfolder`. Se um âmbito mais restrito puder suportar a funcionalidade visível, o âmbito solicitado, os registos de consentimento, a configuração OAuth, o source asset, o asset renderizado e os testes devem ser atualizados antes do lançamento.

Retenção

A DynamicMail conserva dados derivados do Drive apenas enquanto forem necessários para o fluxo de trabalho visível do Drive, para as definições de retenção de documentos do cliente, registos de auditoria, segurança, gestão de litígios ou conformidade jurídica. Os tokens OAuth e metadados de operações do Drive são conservados apenas enquanto forem necessários para operar a integração do Drive ligada ou para preservar registos de auditoria exigidos.

Conteúdo de ficheiros do Drive, ficheiros em cache, metadados, texto de OCR, campos extraídos e dados de documentos derivados devem ser eliminados ou anonimizados quando deixarem de ser necessários para a finalidade comunicada, salvo se uma obrigação jurídica, de segurança, de auditoria ou de retenção do cliente exigir retenção contínua.

Eliminação

Um utilizador autorizado ou administrador do cliente pode solicitar a eliminação de dados em cache derivados da Google, ficheiros do Drive importados, texto extraído e registos de documentos derivados. A DynamicMail deve eliminar ou anonimizar os dados solicitados quando tal for permitido pelas definições de retenção do cliente e pela lei aplicável.

Eliminar registos importados da DynamicMail não elimina necessariamente o ficheiro original do Google Drive. A DynamicMail deve modificar, mover para o lixo ou eliminar ficheiros originais do Drive apenas quando um utilizador autorizado solicitar explicitamente essa ação do Drive através de um fluxo visível do produto e a ação for permitida pela política do cliente e pela lei aplicável.

Revogação e desligação

O cliente pode desligar o Google Drive na DynamicMail. Após a desligação ou a revogação local do consentimento, a DynamicMail deve deixar de utilizar tokens OAuth armazenados para o Google Drive e deve deixar de ler, escrever, transferir, carregar, modificar ou eliminar ficheiros adicionais do Drive da conta ligada.

O proprietário da Conta Google também pode revogar a autorização da aplicação nas definições da Conta Google. Se a autorização da Google for revogada, a DynamicMail deve parar o acesso à API do Drive quando a atualização de tokens ou as chamadas à API falharem, e a ligação deve ser apresentada como desligada ou a exigir nova ligação.

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

Utilização de IA, OCR e extração

A DynamicMail pode utilizar OCR, análise, classificação, resumos e outro tratamento assistido por IA sobre conteúdo e metadados de ficheiros derivados do Drive apenas para fornecer ou melhorar o fluxo de trabalho visível de documentos do Drive solicitado pelo cliente. Dados do Drive e dados derivados não devem ser utilizados para criar, treinar ou melhorar um modelo geral de aprendizagem automática ou IA fora da funcionalidade solicitada pelo cliente.

Os resultados assistidos por IA podem estar incorretos. A DynamicMail deve apresentar os dados extraídos como saída de fluxo de trabalho que utilizadores autorizados podem rever, corrigir, aprovar, rejeitar ou eliminar de acordo com o fluxo do produto.

Acesso de suporte e acesso humano

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

- o utilizador tiver solicitado explicitamente suporte que exige acesso a dados específicos;
- o acesso for necessário para investigação de segurança, prevenção de abuso ou resposta a incidentes;
- o acesso for necessário para cumprir a lei, processo legal ou uma instrução vinculativa do cliente;
- os dados estiverem agregados ou anonimizados para operações internas e nenhum conteúdo do Drive de um utilizador específico for legível.

O acesso de suporte deve basear-se no menor privilégio necessário, ser limitado no tempo quando praticável e ser registado para fins de auditoria.

É material localizado de implementação e revisão, não aconselhamento jurídico final. Não deve ser apresentado como tendo aprovação da Google, aprovação de consultor jurídico externo ou autorização de produção para âmbitos restritos sem prova separada de revisão.

Referências

- 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>