

Termos de acesso a dados do Gmail somente leitura

Estes termos explicam o acesso restrito ao Gmail inbound que a DynamicMail solicita para `https://www.googleapis.com/auth/gmail.readonly` quando um usuário autorizado ou administrador do cliente conecta o Gmail inbound para ingestão de documentos.

Este ativo cobre apenas o Gmail inbound. Ele não deve ser usado como termos completos de acesso a dados do Google Workspace para o Google Drive.

Escopo

A DynamicMail solicita `https://www.googleapis.com/auth/gmail.readonly` somente quando um usuário autorizado ou administrador do cliente conecta o Gmail inbound para ingestão de documentos. O escopo permite que a DynamicMail visualize mensagens e configurações do Gmail da conta Google conectada. A DynamicMail usa o escopo para processamento inbound somente leitura e não o usa para enviar, modificar, excluir, arquivar, rotular ou mover mensagens do Gmail.

Os escopos de identidade do Google Sign-In, como `openid`, `email` e `profile`, são separados deste consentimento de acesso a dados do Gmail. Entrar com o Google não significa aceitar o acesso ao Gmail inbound.

Dados que a DynamicMail pode acessar

Quando o Gmail inbound está conectado, a DynamicMail pode acessar os dados do Gmail necessários para localizar e processar documentos comerciais inbound, incluindo:

- IDs de mensagens, IDs de conversas, IDs de histórico, referências de marcadores e cursores de sincronização;
- remetente, destinatário, assunto, data, cabeçalhos e outros metadados da mensagem;
- corpos de mensagens e trechos necessários para identificar o contexto do documento;
- anexos e arquivos inline que podem conter faturas, avisos, contratos, recibos ou outros documentos do cliente;
- configurações do Gmail somente quando a API do Gmail as exigir para o escopo `readonly` ou para o comportamento de sincronização da conta;
- dados derivados criados a partir do conteúdo do Gmail, 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 nem processar dados do Gmail que não estejam relacionados ao recurso visível de ingestão inbound de documentos.

Por que a DynamicMail usa dados do Gmail

A DynamicMail usa dados do Gmail readonly para fornecer a fonte Gmail inbound selecionada pelo cliente. As finalidades previstas são:

- detectar mensagens inbound que possam conter documentos comerciais do cliente;
- importar anexos ou conteúdo de mensagens que o cliente escolha processar;
- extrair, classificar e encaminhar documentos nos fluxos de trabalho da DynamicMail;
- reconciliar o estado de sincronização para que a mesma mensagem não seja importada repetidamente;
- exibir o status de conexão, sincronização e processamento para usuários autorizados do cliente;
- realizar atividades de suporte, segurança, auditoria e conformidade legal permitidas pelas políticas aplicáveis e pelo acordo com o cliente.

A DynamicMail não deve vender dados do Gmail, 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.

Retenção

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

O conteúdo bruto de mensagens do Gmail, anexos 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, anexos 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 e-mail ou anexo original do Gmail, porque o escopo Gmail readonly não concede à DynamicMail

permissão para modificar ou excluir mensagens do Gmail.

Revogação e desconexão

O cliente pode desconectar o Gmail inbound na DynamicMail. Após a desconexão ou a revogação local do consentimento, a DynamicMail deve parar de usar tokens OAuth armazenados para o Gmail inbound e deve parar de ler mensagens adicionais do Gmail 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 Gmail 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 de mensagens e anexos derivados do Gmail somente para fornecer ou melhorar o fluxo visível de documentos inbound solicitado pelo cliente. Dados do Gmail 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 mensagens específicas do Gmail, anexos, texto extraído ou dados derivados do Gmail, 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 Gmail 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>
- 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>