Checklist de GDPR para Ferramentas de Reunião com IA em 2026 (Guia de Avaliação de Fornecedores)

Checklist do lado do comprador para avaliar ferramentas de reunião com IA sob o GDPR: DPA e Artigo 28, Cláusulas Contratuais Padrão da UE, Avaliações de Impacto de Transferência, Medidas Técnicas/Organizacionais, transparência de subprocessadores e suas obrigações como controlador.

Publicado por Julian Pscheid · 7 de dezembro de 2025 · Atualizado 1 de maio de 2026
Ler este artigo online: https://www.hedy.ai/pt/post/gdpr-checklist-ai-meeting-tools/

Quatro colegas tendo uma discussão focada ao redor de uma mesa de conferência com o horizonte da cidade atrás deles

Resposta rápida Um guia do comprador para avaliar ferramentas de reunião com IA sob o GDPR — cobre DPA/Artigo 28, Cláusulas Contratuais Padrão da UE e Avaliações de Impacto de Transferência, Medidas Técnicas/Organizacionais, transparência de subprocessadores e suas obrigações do lado do controlador (base legal, transparência, DPIA, direitos dos titulares de dados). Use como checklist de fornecedor antes da aprovação de compras.

Um guia prático para profissionais que querem usar assistentes de reunião com IA sem criar dores de cabeça de conformidade. Para uma avaliação comparativa de ferramentas específicas, veja nosso guia detalhado sobre a melhor ferramenta de reunião com IA em conformidade com o GDPR (/post/best-gdpr-compliant-ai-meeting-tool-record-transcribe-eu-data-protection/) .

Usar IA para capturar insights de reuniões, gerar resumos e acompanhar itens de ação se tornou prática padrão para profissionais do conhecimento. Mas se você está sujeito ao GDPR — seja por estar baseado na UE, trabalhar com clientes da UE ou processar dados de residentes da UE — você precisa pensar cuidadosamente sobre como essas ferramentas tratam dados pessoais.

Este checklist ajuda você a avaliar qualquer ferramenta de reunião com IA e garantir que seu uso permaneça em conformidade. Também incluímos orientações sobre o que você precisa fazer da sua parte, porque mesmo a ferramenta mais consciente de privacidade não pode lidar com todas as suas obrigações GDPR por você.

Parte 1: Avaliando Sua Ferramenta de Reunião com IA

Antes de adotar qualquer assistente de reunião com IA, verifique esses fundamentos:

Acordos de Processamento de Dados

O que procurar:

• Um Adendo de Processamento de Dados (DPA) que atenda aos requisitos do Artigo 28 do GDPR

• Documentação clara de quais dados são processados e para quais fins

• Papéis definidos (você como controlador, o provedor da ferramenta como processador)

Por que importa: Um DPA é obrigatório quando um fornecedor processa dados pessoais em seu nome (Artigo 28). Isso é separado da sua base legal do Artigo 6 para o processamento em si — você precisa de ambos. Usar um processador sem um acordo em conformidade com o Artigo 28 não está em conformidade, independentemente da sua base legal.

Transferências Internacionais de Dados

Se o provedor da sua ferramenta está baseado fora da UE (a maioria é dos EUA), você precisa de salvaguardas adicionais:

O que procurar:

• Cláusulas Contratuais Padrão (SCCs) da UE incorporadas no acordo

• Uma Avaliação de Impacto de Transferência (TIA) documentando a situação legal no país de destino e quaisquer medidas suplementares

• Informações claras sobre quais subprocessadores tratam seus dados e onde

• A opção de verdadeira residência de dados na UE (/post/eu-data-residency/) — seus dados de conversa armazenados em infraestrutura fisicamente localizada na União Europeia

Por que importa: A decisão Schrems II invalidou o EU-US Privacy Shield. Ferramentas que transferem dados para os EUA tipicamente dependem de SCCs, mas estas requerem avaliação caso a caso e, quando necessário, medidas suplementares para garantir proteção adequada.

Medidas Técnicas e Organizacionais (TOMs)

O que procurar:

• Documentação de medidas de segurança (criptografia, controles de acesso, etc.)

• Informações sobre onde e como os dados são armazenados

• Políticas de retenção de dados — por quanto tempo os dados são mantidos?

• Opções de processamento local/no dispositivo vs processamento na nuvem

Por que importa: Você precisa verificar que seu processador tem medidas de segurança apropriadas para a sensibilidade dos dados que você está processando.

Considerações Específicas de IA

O que procurar:

• Confirmação de que seus dados não são usados para treinar modelos de IA
• Políticas claras de retenção de dados com subprocessadores de IA (idealmente retenção zero)
• Transparência sobre quais serviços de IA processam seus dados

Por que importa: Muitas ferramentas de IA enviam dados de conversa para serviços de IA terceirizados. Você precisa de visibilidade sobre quem processa seus dados e em quais termos. Embora o GDPR não exija períodos de retenção específicos, os princípios de minimização de dados favorecem retenção mais curta, e compromissos de retenção zero dos subprocessadores de IA reduzem sua exposição ao risco.

Transparência de Subprocessadores

O que procurar:

• Uma lista completa de subprocessadores com seus propósitos e localizações
• Processo de notificação para mudanças de subprocessadores
• Capacidade de se opor a novos subprocessadores

Por que importa: O Artigo 28(2) exige que os processadores obtenham autorização do controlador para subprocessadores. Você precisa de visibilidade sobre todos que tocam seus dados e a capacidade de avaliar se seu envolvimento é apropriado.

Parte 2: Suas Responsabilidades como Controlador de Dados

Mesmo com uma ferramenta totalmente em conformidade, você tem obrigações que nenhum software pode cumprir por você:

Antes de Começar a Gravar

Base Legal

• Identifique sua base legal para processamento sob o Artigo 6 do GDPR (interesse legítimo, consentimento, execução de contrato, etc.)
• Documente essa base e esteja preparado para explicá-la se solicitado
• Nota: Consentimento é uma opção, mas interesses legítimos ou necessidade contratual podem ser apropriados dependendo do seu contexto

Transparência e Notificação

• Informe todos os participantes da reunião que ferramentas de IA processarão a conversa
• Explique o que será capturado, como será processado e quem terá acesso
• Forneça essas informações de forma clara e antes de o processamento começar
• Para scripts práticos que atendem tanto à transparência do GDPR quanto à maioria das leis locais de gravação, veja Como pedir permissão para gravar uma reunião (/post/ask-permission-to-record-meeting-consent-scripts/)

Leis de Gravação (Separadas do GDPR)

• Verifique as leis locais sobre gravação de conversas — muitas jurisdições exigem consentimento dos participantes independentemente do GDPR

• Esses requisitos variam por país e podem ser mais rigorosos que o próprio GDPR

• Em caso de dúvida, obter consentimento explícito atende tanto aos requisitos de transparência do GDPR quanto à maioria das leis locais de gravação

Avaliação de Risco

• Considere se uma Avaliação de Impacto de Proteção de Dados (DPIA) é necessária

• DPIAs são obrigatórias para processamento que provavelmente resultará em alto risco para os direitos e liberdades dos indivíduos

• Fatores que podem indicar alto risco incluem: processamento em larga escala, dados sensíveis, novas tecnologias e monitoramento sistemático

• Mesmo quando não estritamente necessárias, DPIAs são boas práticas para processamento baseado em IA e ajudam a demonstrar responsabilidade

Conformidade Contínua

Atualizações da Política de Privacidade

• Atualize sua política de privacidade para refletir o uso de ferramentas de reunião com IA

• Inclua: quais dados são coletados, propósitos, base legal, períodos de retenção, terceiros envolvidos e direitos dos titulares de dados

Direitos dos Titulares de Dados

• Estabeleça processos para lidar com solicitações de acesso (as pessoas podem perguntar quais dados você possui sobre elas)

• Habilite solicitações de exclusão — você precisa ser capaz de remover os dados de alguém dos seus registros de reunião

• Documente como você lidará com solicitações de objeção, particularmente se dependendo de interesses legítimos

Retenção e Exclusão

• Defina por quanto tempo você manterá dados de reunião com base nos seus propósitos declarados

• Implemente cronogramas regulares de exclusão

• Os princípios de minimização de dados significam que você não deve manter dados por mais tempo do que o necessário

Manutenção de Registros

• Mantenha registros de atividades de processamento conforme exigido pelo Artigo 30

• Documente suas medidas e decisões de conformidade

Revisão Anual

A conformidade com o GDPR não é uma tarefa única:

• Revise os termos atualizados da sua ferramenta, DPA e lista de subprocessadores pelo menos anualmente

• Reavalie sua base legal se seus casos de uso mudarem

• Atualize sua DPIA se as atividades de processamento mudarem significativamente
• Verifique se seus cronogramas de retenção estão sendo seguidos

Parte 3: Decisões de Configuração

A maioria das ferramentas de reunião com IA oferece vários recursos que afetam sua postura de privacidade. Para cada recurso que você habilitar, considere as implicações de conformidade: (Para orientações de configuração específicas do Hedy — o que cada configuração faz e perfis recomendados para advogados, profissionais de saúde e coaches — veja Configurações de Privacidade do Hedy Explicadas (/post/ai-meeting-privacy-settings-explained/) .)

.gdpr-table { width: 100%; border-collapse: collapse; margin: 1.5em 0; font-size: 1rem; } .gdpr-table th, .gdpr-table td { padding: 12px 16px; text-align: left; border-bottom: 1px solid #e2e8f0; } .gdpr-table th { background-color: #f8fafc; font-weight: 600; color: #1e293b; } .gdpr-table tr:hover { background-color: #f8fafc; } .gdpr-table td:first-child { font-weight: 500; color: #334155; }

Recurso | Consideração de Privacidade

Sincronização em nuvem | Os dados saem do seu dispositivo e são armazenados nos servidores do provedor
Coaching/sugestões de IA ao vivo | Transmissão de dados em tempo real para serviços de IA
Resumos por e-mail | Conteúdo da reunião transmitido via e-mail (geralmente não criptografado)
Armazenamento de gravação de áudio | Gravações de voz são dados pessoais; veja nota abaixo sobre dados biométricos
Compartilhamento/colaboração | Amplia o acesso aos dados para partes adicionais
Integrações via API | Dados fluem para sistemas terceirizados adicionais

Nota sobre gravações de áudio: Gravações de voz são dados pessoais. Elas podem se qualificar como dados biométricos de categoria especial sob o Artigo 9 se processadas com o propósito de identificar exclusivamente uma pessoa (ex.: análise de impressão vocal, sistemas de identificação de falantes). Gravações de reuniões padrão usadas para transcrição e anotações tipicamente não se enquadram nessa categoria, mas se você está usando recursos de identificação de voz, os requisitos do Artigo 9 se aplicam.

Princípio geral: Habilite apenas o que você precisa. Cada recurso adicional expande sua pegada de processamento de dados e requer justificativa sob os princípios de minimização de dados.

Categorias Especiais de Dados

Se suas reuniões envolvem dados sensíveis sob o Artigo 9 do GDPR — informações de saúde, opiniões políticas, crenças religiosas, dados processados para identificação biométrica exclusiva, etc. — você precisa de proteções aprimoradas:

• Uma base legal específica sob o Artigo 6 E uma condição sob o Artigo 9(2)
• Consentimento explícito é comumente usado, mas outras condições podem se aplicar dependendo do contexto
• Medidas de segurança mais fortes apropriadas à sensibilidade
• DPIA provavelmente necessária
• Considere se os recursos de nuvem são apropriados dado o perfil de risco

Parte 4: Implementação Prática

Exemplo de Linguagem de Notificação e Consentimento

Antes de iniciar qualquer reunião gravada:

> *"Gostaria de usar um assistente de IA para ajudar a capturar notas e insights da nossa conversa. Isso significa que nossa discussão será transcrita e analisada por IA. O transcrito fica sob meu controle e não será usado para treinar nenhum modelo de IA. Você está confortável com isso?"*

Aguarde a confirmação antes de começar. Essa abordagem satisfaz tanto os requisitos de transparência do GDPR quanto a maioria das leis locais de consentimento para gravação.

Adição ao Convite de Calendário

> *"Esta reunião terá suporte de anotações por IA. Se você tiver preocupações sobre isso, por favor me avise antes da reunião."*

Nota: Isso fornece aviso prévio, o que é uma boa prática. Dependendo da sua base legal e das leis locais de gravação, você ainda pode precisar confirmar o consentimento no início da reunião.

Linguagem para Política de Privacidade (Modelo)

Inclua na sua política de privacidade:

> *Assistência de Reunião com IA Utilizamos ferramentas com IA para transcrever e analisar reuniões com o propósito de [capturar itens de ação / melhorar a comunicação / manter registros precisos] . Este processamento é baseado em [sua base legal, ex.: interesses legítimos na manutenção de registros comerciais precisos / execução de contrato / consentimento] . Os dados da reunião podem ser processados pelo nosso provedor de ferramenta de reunião com IA e seus subprocessadores. Os dados podem ser transferidos para os Estados Unidos sob Cláusulas Contratuais Padrão da UE com medidas suplementares apropriadas. Transcrições e resumos de reuniões são retidos por [X período] e depois excluídos. Você pode solicitar acesso, correção ou exclusão dos seus dados entrando em contato com [dados de contato] .*

Adapte isso à sua situação específica e base legal.

Como o Hedy Lida com a Conformidade GDPR

Construímos o Hedy com privacidade como princípio central, não como algo secundário. Para a explicação completa da conformidade do Hedy com o GDPR (/post/hedy-ai-gdpr-compliance/) — incluindo o DPA, as SCCs e a Avaliação de Impacto de Transferência — consulte o post dedicado. Veja como abordamos os requisitos neste checklist:

Estrutura Contratual

• Adendo de Processamento de Dados com Cláusulas Contratuais Padrão da UE incluído automaticamente com sua conta

• Avaliação de Impacto de Transferência disponível documentando salvaguardas de transferência de dados para os EUA e medidas suplementares

• Documentação completa de Medidas Técnicas e Organizacionais

• Lista transparente de subprocessadores com notificações de mudanças

Arquitetura Focada em Privacidade

• Reconhecimento de fala no dispositivo por padrão — seu áudio nunca sai do dispositivo, a menos que você habilite recursos de nuvem

• Acordos de retenção zero de dados com subprocessadores de IA
• Seus dados nunca são usados para treinar modelos de IA
• Controles granulares: habilite apenas os recursos que você precisa

Documentação de Conformidade

• Documentação completa disponível no nosso Trust Center
• Orientação de conformidade GDPR para usuários (responsabilidades do controlador)
• Certificações SOC 2 Type I e HIPAA em andamento (previstas para Q2 2026)

Controle do Usuário

• Modo apenas local disponível para máxima privacidade
• Exclua seus dados a qualquer momento
• Exporte seus dados para portabilidade
• Configuração de região de proteção de dados da UE para minimizar rastreamento

Acesse nossa documentação completa de conformidade em trust.hedy.ai (https://trust.hedy.ai) .

Perguntas frequentes

Como avalio uma ferramenta de reunião com IA para conformidade com o GDPR?

Verifique quatro coisas: um DPA que atenda ao Artigo 28 (com SCCs da UE se o fornecedor estiver fora da UE), uma Avaliação de Impacto de Transferência documentando leis de proteção de dados dos EUA e medidas suplementares, Medidas Técnicas/Organizacionais documentadas e uma lista completa de subprocessadores com direitos de notificação. Se um fornecedor não consegue fornecer os quatro, ele não está pronto para GDPR no seu negócio.

Que perguntas devo fazer a um fornecedor sobre GDPR?

Cinco perguntas básicas: (1) Você pode fornecer um DPA com cláusulas do Artigo 28? (2) Onde os dados são armazenados fisicamente, e vocês oferecem residência na UE? (3) As Cláusulas Contratuais Padrão da UE estão incorporadas para qualquer transferência fora da UE, e uma TIA está disponível? (4) Quem são seus subprocessadores e onde eles operam? (5) Meus dados são usados em algum momento para treinar modelos de IA? Se alguma resposta estiver faltando, questione.

O que é uma Cláusula Contratual Padrão e eu preciso de uma?

Cláusulas Contratuais Padrão (SCCs) são modelos contratuais aprovados pela UE que vinculam um importador de dados fora da UE a proteções de nível UE quando dados pessoais são transferidos para fora da UE. Após Schrems II, fornecedores baseados nos EUA normalmente dependem de SCCs mais medidas suplementares documentadas em uma Avaliação de Impacto de Transferência. Se seu fornecedor está nos EUA e processa dados pessoais da UE, sim — você precisa de SCCs em vigor.

Preciso de uma Avaliação de Impacto de Proteção de Dados para ferramentas de reunião com IA?

Uma DPIA é obrigatória sob o Artigo 35 se o processamento provavelmente resultar em alto risco para titulares de dados — gatilhos típicos incluem monitoramento sistemático, processamento em larga escala, dados sensíveis ou novas tecnologias. Gravação baseada em IA frequentemente aciona um ou

mais gatilhos. Mesmo quando não é estritamente obrigatória, uma DPIA é boa prática e demonstra responsabilidade.

Quais são minhas responsabilidades como controlador de dados ao usar ferramentas de reunião com IA?

Estabelecer uma base legal sob o Artigo 6 (interesse legítimo, consentimento, execução de contrato), fornecer avisos de transparência aos participantes antes da gravação, manter registros de atividades de processamento do Artigo 30, conduzir uma DPIA quando exigida, lidar com direitos dos titulares de dados (acesso, exclusão, objeção) e atualizar sua política de privacidade. O fornecedor lida com as obrigações do lado do processador; você lida com as do lado do controlador.

Dúvidas?

A conformidade com o GDPR pode parecer complexa, mas não precisa ser avassaladora. Se você tiver dúvidas sobre usar o Hedy de forma compatível com o GDPR, entre em contato conosco em privacy@hedy.ai (mailto:privacy@hedy.ai) ou consulte nossa documentação de ajuda (https://help.hedy.bot) .

Para questões de conformidade complexas específicas à sua organização, recomendamos consultar um profissional qualificado de proteção de dados ou seu Encarregado de Proteção de Dados.

Este guia fornece informações gerais sobre conformidade GDPR para ferramentas de reunião com IA. Não constitui aconselhamento jurídico e não deve ser utilizado como tal. Os requisitos podem variar com base na sua situação específica, jurisdição e natureza dos dados que você processa. As leis locais sobre gravação de conversas podem impor requisitos adicionais além do GDPR.
