

Checklist RGPD pour les outils de réunion IA en 2026 (guide d'évaluation des fournisseurs)

Checklist côté acheteur pour évaluer les outils de réunion IA au regard du RGPD : DPA et Article 28, Clauses Contractuelles Types de l'UE, TIA, Mesures Techniques et Organisationnelles, transparence sur les sous-traitants et vos obligations de responsable du traitement.

Publié par Julian Pscheid · 7 décembre 2025 · Mis à jour 1 mai 2026

[Lire cet article en ligne: https://www.hedy.ai/fr/post/gdpr-checklist-ai-meeting-tools/](https://www.hedy.ai/fr/post/gdpr-checklist-ai-meeting-tools/)



Quatre collègues en discussion concentrée autour d'une table de conférence avec le panorama d'une ville en arrière-plan

Réponse rapide Un guide d'achat pour évaluer les outils de réunion IA au regard du RGPD : DPA/Article 28, Clauses Contractuelles Types de l'UE et TIA, Mesures Techniques et Organisationnelles, transparence sur les sous-traitants et vos obligations côté responsable du traitement (base juridique, transparence, AIPD, droits des personnes concernées). Utilisez-le comme checklist fournisseur avant la validation par les achats.

Un guide pratique pour les professionnels qui souhaitent utiliser des assistants de réunion alimentés par l'IA sans créer de problèmes de conformité. Pour une évaluation comparative d'outils spécifiques, consultez notre guide approfondi du meilleur outil de réunion IA conforme au RGPD (/post/best-gdpr-compliant-ai-meeting-tool-record-transcribe-eu-data-protection/).

Utiliser l'IA pour capturer les informations de réunion, générer des résumés et suivre les actions à mener est devenu une pratique courante pour les travailleurs du savoir. Mais si vous êtes soumis au RGPD — que vous soyez basé dans l'UE, que vous travailliez avec des clients européens ou que vous traitiez les données de résidents de l'UE — vous devez réfléchir attentivement à la manière dont ces outils gèrent les données personnelles.

Cette checklist vous aide à évaluer tout outil de réunion IA et à garantir que votre utilisation reste conforme. Nous avons également inclus des conseils sur ce que vous devez faire de votre côté, car même l'outil le plus soucieux de la vie privée ne peut pas assumer toutes vos obligations RGPD à votre place.

Partie 1 : Évaluer votre outil de réunion IA

Avant d'adopter tout assistant de réunion IA, vérifiez ces fondamentaux :

Accords de traitement des données

Ce qu'il faut rechercher :

- Un Avenant au Traitement des Données (DPA) conforme aux exigences de l'Article 28 du RGPD
- Une documentation claire sur les données traitées et les finalités
- Des rôles définis (vous en tant que responsable du traitement, le fournisseur de l'outil en tant que sous-traitant)

Pourquoi c'est important : Un DPA est requis lorsqu'un prestataire traite des données personnelles pour votre compte (Article 28). C'est distinct de votre base juridique au titre de l'Article 6 pour le traitement lui-même — vous avez besoin des deux. Utiliser un sous-traitant sans accord conforme à l'Article 28 est non conforme, quelle que soit votre base juridique.

Transferts internationaux de données

Si votre fournisseur d'outil est basé hors de l'UE (la plupart sont basés aux États-Unis), vous avez besoin de garanties supplémentaires :

Ce qu'il faut rechercher :

- Les Clauses Contractuelles Types (SCCs) de l'UE intégrées dans l'accord
- Une Analyse d'Impact du Transfert (TIA) documentant la situation juridique dans le pays de destination et les mesures supplémentaires
- Des informations claires sur les sous-traitants qui traitent vos données et où
- L'option d'une vraie résidence des données dans l'UE ([/post/eu-data-residency/](#)) — vos données de conversation stockées sur une infrastructure physiquement située dans l'Union européenne

Pourquoi c'est important : L'arrêt Schrems II a invalidé le EU-US Privacy Shield. Les outils qui transfèrent des données aux États-Unis s'appuient généralement sur les SCCs, mais celles-ci nécessitent une évaluation au cas par cas et, si nécessaire, des mesures supplémentaires pour garantir une protection adéquate.

Mesures Techniques et Organisationnelles (TOMs)

Ce qu'il faut rechercher :

- Documentation des mesures de sécurité (chiffrement, contrôles d'accès, etc.)

- Informations sur l'emplacement et les modalités de stockage des données
- Politiques de conservation des données — combien de temps les données sont-elles conservées ?
- Options de traitement local/sur l'appareil vs traitement cloud

Pourquoi c'est important : Vous devez vérifier que votre sous-traitant dispose de mesures de sécurité appropriées à la sensibilité des données que vous traitez.

Considérations spécifiques à l'IA

Ce qu'il faut rechercher :

- Confirmation que vos données ne sont pas utilisées pour entraîner des modèles IA
- Politiques claires de conservation des données chez les sous-traitants IA (idéalement zéro conservation)
- Transparence sur les services IA qui traitent vos données

Pourquoi c'est important : De nombreux outils IA envoient les données de conversation à des services IA tiers. Vous avez besoin de visibilité sur qui traite vos données et selon quelles conditions. Bien que le RGPD n'impose pas de durées de conservation spécifiques, les principes de minimisation des données favorisent des durées plus courtes, et les engagements de zéro conservation des sous-traitants IA réduisent votre exposition au risque.

Transparence sur les sous-traitants

Ce qu'il faut rechercher :

- Une liste complète des sous-traitants avec leurs finalités et localisations
- Un processus de notification en cas de changement de sous-traitant
- La possibilité de s'opposer à de nouveaux sous-traitants

Pourquoi c'est important : L'Article 28(2) exige que les sous-traitants obtiennent l'autorisation du responsable du traitement pour les sous-traitants ultérieurs. Vous avez besoin de visibilité sur tous ceux qui touchent vos données et la capacité d'évaluer si leur implication est appropriée.

Partie 2 : Vos responsabilités en tant que responsable du traitement

Même avec un outil entièrement conforme, vous avez des obligations qu'aucun logiciel ne peut remplir à votre place :

Avant de commencer à enregistrer

Base juridique

- Identifiez votre base juridique pour le traitement au titre de l'Article 6 du RGPD (intérêt légitime, consentement, exécution d'un contrat, etc.)
- Documentez cette base et soyez prêt à l'expliquer si on vous le demande
- Note : le consentement est une option, mais les intérêts légitimes ou la nécessité contractuelle peuvent être appropriés selon votre contexte

Transparence et information

- Informez tous les participants à la réunion que des outils IA traiteront la conversation
- Expliquez ce qui sera capturé, comment ce sera traité, et qui y aura accès

- Fournissez ces informations clairement et avant le début du traitement
- Pour des scripts pratiques qui satisfont à la fois la transparence du RGPD et la plupart des lois locales sur l'enregistrement, consultez Comment demander la permission d'enregistrer une réunion (/post/ask-permission-to-record-meeting-consent-scripts/)

Lois sur l'enregistrement (distinctes du RGPD)

- Vérifiez les lois locales sur l'enregistrement des conversations — de nombreuses juridictions exigent le consentement des participants indépendamment du RGPD
- Ces exigences varient selon les pays et peuvent être plus strictes que le RGPD lui-même
- En cas de doute, obtenir un consentement explicite répond à la fois aux exigences de transparence du RGPD et à la plupart des lois locales sur l'enregistrement

Évaluation des risques

- Déterminez si une Analyse d'Impact relative à la Protection des Données (AIPD) est requise
- Les AIPD sont obligatoires pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des individus
- Les facteurs pouvant indiquer un risque élevé comprennent : le traitement à grande échelle, les données sensibles, les nouvelles technologies et la surveillance systématique
- Même lorsqu'elle n'est pas strictement requise, l'AIPD est une bonne pratique pour le traitement basé sur l'IA et aide à démontrer la responsabilité

Conformité continue

Mises à jour de la politique de confidentialité

- Mettez à jour votre politique de confidentialité pour refléter votre utilisation d'outils de réunion IA
- Incluez : les données collectées, les finalités, la base juridique, les durées de conservation, les tiers impliqués et les droits des personnes concernées

Droits des personnes concernées

- Établissez des processus pour traiter les demandes d'accès (les personnes peuvent demander quelles données vous détenez à leur sujet)
- Permettez les demandes de suppression — vous devez être en mesure de supprimer les données d'une personne de vos enregistrements de réunion
- Documentez comment vous gérerez les demandes d'opposition, en particulier si vous vous appuyez sur les intérêts légitimes

Conservation et suppression

- Définissez combien de temps vous conserverez les données de réunion en fonction de vos finalités déclarées
- Mettez en place des calendriers de suppression réguliers
- Les principes de minimisation des données signifient que vous ne devriez pas conserver les données plus longtemps que nécessaire

Tenue de registres

- Tenez des registres des activités de traitement comme requis par l'Article 30
- Documentez vos mesures et décisions de conformité

Revue annuelle

La conformité RGPD n'est pas une tâche ponctuelle :

- Réviser les conditions mises à jour de votre outil, le DPA et la liste des sous-traitants au moins une fois par an
- Réévaluez votre base juridique si vos cas d'usage changent
- Mettez à jour votre AIPD si les activités de traitement changent significativement
- Vérifiez que vos calendriers de conservation sont respectés

Partie 3 : Décisions de configuration

La plupart des outils de réunion IA offrent diverses fonctionnalités qui affectent votre posture de confidentialité. Pour chaque fonctionnalité que vous activez, considérez les implications de conformité. (Pour des conseils de configuration propres à Hedy — ce que fait chaque paramètre et les profils recommandés pour les avocats, les professionnels de santé et les coachs — consultez Les paramètres de confidentialité de Hedy expliqués (/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; }
```

Fonctionnalité | Considération de confidentialité

Synchronisation cloud | Les données quittent votre appareil et sont stockées sur les serveurs du fournisseur

Coaching/suggestions IA en direct | Transmission de données en temps réel vers les services IA

Résumés par e-mail | Contenu de réunion transmis par e-mail (généralement non chiffré)

Stockage d'enregistrements audio | Les enregistrements vocaux sont des données personnelles ; voir la note ci-dessous sur les données biométriques

Partage/collaboration | Étend l'accès aux données à des parties supplémentaires

Intégrations API | Les données transitent vers des systèmes tiers supplémentaires

Note sur les enregistrements audio : Les enregistrements vocaux sont des données personnelles. Ils peuvent être qualifiés de données biométriques de catégorie spéciale au titre de l'Article 9 s'ils sont traités dans le but d'identifier de manière unique une personne (ex. : analyse d'empreinte vocale, systèmes d'identification du locuteur). Les enregistrements de réunion standard utilisés pour la transcription et la prise de notes ne tombent généralement pas dans cette catégorie, mais si vous utilisez des fonctionnalités d'identification vocale, les exigences de l'Article 9 s'appliquent.

Principe général : N'activez que ce dont vous avez besoin. Chaque fonctionnalité supplémentaire élargit votre empreinte de traitement des données et nécessite une justification selon les principes de minimisation des données.

Catégories spéciales de données

Si vos réunions impliquent des données sensibles au sens de l'Article 9 du RGPD — informations de santé, opinions politiques, croyances religieuses, données traitées pour l'identification biométrique unique, etc. — vous avez besoin de protections renforcées :

- Une base juridique spécifique au titre de l'Article 6 ET une condition au titre de l'Article 9(2)
- Le consentement explicite est couramment utilisé, mais d'autres conditions peuvent s'appliquer selon le contexte
- Des mesures de sécurité renforcées adaptées à la sensibilité
- AIPD probablement requise

- Réfléchissez à l'adéquation des fonctionnalités cloud au regard du profil de risque

Partie 4 : Mise en pratique

Exemple de formulation pour l'information et le consentement

Avant de démarrer toute réunion enregistrée :

« Je souhaiterais utiliser un assistant IA pour capturer les notes et les informations clés de notre conversation. Cela signifie que notre discussion sera transcrite et analysée par l'IA. La transcription reste sous mon contrôle et ne sera pas utilisée pour entraîner des modèles IA. Cela vous convient-il ? »

Attendez la confirmation avant de démarrer. Cette approche satisfait à la fois les exigences de transparence du RGPD et la plupart des lois locales sur le consentement à l'enregistrement.

Ajout à l'invitation de calendrier

« Cette réunion sera accompagnée par une prise de notes IA. Si vous avez des préoccupations à ce sujet, veuillez me contacter avant la réunion. »

Note : Cela fournit un préavis, ce qui est une bonne pratique. Selon votre base juridique et les lois locales sur l'enregistrement, vous pourriez encore devoir confirmer le consentement au début de la réunion.

Formulation pour la politique de confidentialité (modèle)

Incluez dans votre politique de confidentialité :

Assistance par IA pour les réunions Nous utilisons des outils alimentés par l'IA pour transcrire et analyser les réunions dans le but de [capturer les actions à mener / améliorer la communication / maintenir des archives précises]. Ce traitement est fondé sur [votre base juridique, ex. : intérêts légitimes dans le maintien d'archives d'entreprise précises / exécution d'un contrat / consentement]. Les données de réunion peuvent être traitées par notre fournisseur d'outil de réunion IA et ses sous-traitants. Les données peuvent être transférées aux États-Unis en vertu des Clauses Contractuelles Types de l'UE avec des mesures supplémentaires appropriées. Les transcriptions et résumés de réunion sont conservés pendant [X durée] puis supprimés. Vous pouvez demander l'accès à vos données, leur rectification ou leur suppression en contactant [coordonnées].

Adaptez ce texte à votre situation spécifique et à votre base juridique.

Comment Hedy gère la conformité RGPD

Nous avons conçu Hedy avec la confidentialité comme principe fondamental, pas comme un ajout après coup. Pour le détail complet de la conformité RGPD de Hedy (</post/hedy-ai-gdpr-compliance/>) — y compris le DPA, les SCCs et la TIA — consultez l'article dédié. Voici comment nous avons répondu aux exigences de cette checklist :

Cadre contractuel

- Avenant au Traitement des Données avec les Clauses Contractuelles Types de l'UE inclus automatiquement avec votre compte
- Analyse d'Impact du Transfert disponible documentant les garanties et mesures supplémentaires pour les transferts de données aux États-Unis

- Documentation complète des Mesures Techniques et Organisationnelles
- Liste transparente des sous-traitants avec notifications de changement

Architecture axée sur la confidentialité

- Reconnaissance vocale sur l'appareil par défaut — votre audio ne quitte jamais votre appareil sauf si vous activez les fonctionnalités cloud
- Accords de zéro conservation avec les sous-traitants IA
- Vos données ne sont jamais utilisées pour entraîner des modèles IA
- Contrôles granulaires : n'activez que les fonctionnalités dont vous avez besoin

Documentation de conformité

- Documentation complète disponible dans notre Trust Center
- Guide de conformité RGPD pour les utilisateurs (responsabilités du responsable du traitement)
- Certifications SOC 2 Type I et HIPAA en cours (attendues T2 2026)

Contrôle utilisateur

- Mode local uniquement disponible pour une confidentialité maximale
- Supprimez vos données à tout moment
- Exportez vos données pour la portabilité
- Paramètre de région de protection des données UE pour minimiser le suivi

Accédez à notre documentation de conformité complète sur trust.hedy.ai (<https://trust.hedy.ai>) .

Foire aux questions

Comment évaluer un outil de réunion IA pour la conformité RGPD ?

Vérifiez quatre éléments : un DPA conforme à l'Article 28 (avec SCCs de l'UE si le fournisseur est hors UE), une TIA documentant les lois américaines de protection des données et les mesures supplémentaires, des Mesures Techniques et Organisationnelles documentées, et une liste complète des sous-traitants avec droits de notification. Si un fournisseur ne peut pas produire les quatre, il n'est pas prêt pour le RGPD dans votre entreprise.

Quelles questions dois-je poser à un fournisseur au sujet du RGPD ?

Cinq questions de base : (1) Pouvez-vous fournir un DPA avec les clauses de l'Article 28 ? (2) Où les données sont-elles physiquement stockées, et proposez-vous la résidence dans l'UE ? (3) Les Clauses Contractuelles Types de l'UE sont-elles intégrées pour tout transfert hors UE, et une TIA est-elle disponible ? (4) Qui sont vos sous-traitants et où opèrent-ils ? (5) Mes données sont-elles déjà utilisées pour entraîner des modèles IA ? Si une réponse manque, insistez.

Qu'est-ce qu'une Clause Contractuelle Type et en ai-je besoin ?

Les Clauses Contractuelles Types (SCCs) sont des modèles contractuels approuvés par l'UE qui obligent un importateur de données hors UE à respecter des protections de niveau européen lorsque des données personnelles sont transférées hors de l'UE. Après Schrems II, les fournisseurs basés aux États-Unis s'appuient généralement sur les SCCs plus des mesures supplémentaires documentées dans une TIA. Si votre fournisseur est aux États-Unis et traite des données personnelles européennes, oui : les SCCs doivent être en place.

Ai-je besoin d'une Analyse d'Impact relative à la Protection des Données pour les outils de réunion IA ?

Une AIPD est obligatoire au titre de l'Article 35 si le traitement est susceptible d'engendrer un risque élevé pour les personnes concernées : les déclencheurs typiques incluent la surveillance systématique, le traitement à grande échelle, les données sensibles ou les nouvelles technologies. L'enregistrement basé sur l'IA coche souvent un ou plusieurs de ces critères. Même lorsqu'elle n'est pas strictement requise, une AIPD est une bonne pratique et démontre la responsabilité.

Quelles sont mes responsabilités comme responsable du traitement lorsque j'utilise des outils de réunion IA ?

Établir une base juridique au titre de l'Article 6 (intérêt légitime, consentement, exécution d'un contrat), fournir des informations de transparence aux participants avant l'enregistrement, tenir les registres des activités de traitement de l'Article 30, réaliser une AIPD lorsque requise, gérer les droits des personnes concernées (accès, suppression, opposition) et mettre à jour votre politique de confidentialité. Le fournisseur gère les obligations côté sous-traitant ; vous gérez celles côté responsable du traitement.

Des questions ?

La conformité RGPD peut sembler complexe, mais elle n'a pas à être accablante. Si vous avez des questions sur l'utilisation de Hedy de manière conforme au RGPD, contactez-nous à privacy@hedy.ai (mailto:privacy@hedy.ai) ou consultez notre documentation d'aide (<https://help.hedy.bot>) .

Pour les questions de conformité complexes spécifiques à votre organisation, nous recommandons de consulter un professionnel qualifié de la protection des données ou votre Délégué à la Protection des Données.

Ce guide fournit des informations générales sur la conformité RGPD pour les outils de réunion IA. Il ne constitue pas un avis juridique et ne devrait pas être utilisé comme tel. Les exigences peuvent varier en fonction de votre situation spécifique, de votre juridiction et de la nature des données que vous traitez. Les lois locales sur l'enregistrement des conversations peuvent imposer des exigences supplémentaires au-delà du RGPD.

Hedy AI · Coaching IA en direct pour les conversations importantes

Essayez Hedy gratuitement: <https://www.hedy.ai/fr/downloads/>

<https://www.hedy.ai/fr/post/gdpr-checklist-ai-meeting-tools/>