DSGVO-Checkliste für KI-Meeting-Tools 2026 (Leitfaden zur Anbieterbewertung)

Checkliste für Käufer zur Bewertung von KI-Meeting-Tools unter der DSGVO: AVV und Art. 28, EU-Standardvertragsklauseln, Transfer Impact Assessments, technische/organisatorische Maßnahmen, Unterauftragsverarbeiter-Transparenz und Ihre Pflichten als Verantwortlicher.

Veröffentlicht von Julian Pscheid · 7. Dezember 2025 · Aktualisiert 1. Mai 2026
Diesen Artikel online lesen: https://www.hedy.ai/de/post/gdpr-checklist-ai-meeting-tools/

Vier Kollegen in einer fokussierten Diskussion an einem Konferenztisch mit Stadtpanorama im Hintergrund

Schnelle Antwort Ein Käuferleitfaden zur Bewertung von KI-Meeting-Tools unter der DSGVO — behandelt AVV/Art. 28, EU-Standardvertragsklauseln und Transfer Impact Assessments, technische/organisatorische Maßnahmen, Unterauftragsverarbeiter-Transparenz und Ihre Pflichten als Verantwortlicher (Rechtsgrundlage, Transparenz, DSFA, Betroffenenrechte). Nutzen Sie dies als Anbieter-Checkliste, bevor die Beschaffung freigibt.

Ein praktischer Leitfaden für Fachleute, die KI-gestützte Meeting-Assistenten nutzen möchten, ohne Compliance-Probleme zu verursachen. Für eine vergleichende Bewertung konkreter Tools lesen Sie unsere ausführliche Analyse zum besten DSGVO-konformen KI-Meeting-Tool (/post/best-gdpr-compliant-ai-meeting-tool-record-transcribe-eu-data-protection/) .

Die Nutzung von KI zur Erfassung von Meeting-Erkenntnissen, Generierung von Zusammenfassungen und zum Überblick über Aufgaben ist für Wissensarbeiter zum Standard geworden. Aber wenn Sie der DSGVO unterliegen – ob Sie in der EU ansässig sind, mit EU-Kunden arbeiten oder Daten von EU-Bürgern verarbeiten – müssen Sie sorgfältig überlegen, wie diese Tools mit personenbezogenen Daten

umgehen.

Diese Checkliste hilft Ihnen, jedes KI-Meeting-Tool zu bewerten und sicherzustellen, dass Ihre Nutzung konform bleibt. Wir haben auch Hinweise zu Ihren eigenen Pflichten aufgenommen, denn selbst das datenschutzfreundlichste Tool kann nicht alle Ihre DSGVO-Verpflichtungen für Sie übernehmen.

Teil 1: Bewertung Ihres KI-Meeting-Tools

Bevor Sie einen KI-Meeting-Assistenten einführen, überprüfen Sie diese Grundlagen:

Auftragsverarbeitungsverträge

Worauf Sie achten sollten:

• Ein Auftragsverarbeitungsvertrag (AVV), der den Anforderungen von Art. 28 DSGVO entspricht

• Klare Dokumentation, welche Daten zu welchen Zwecken verarbeitet werden

• Definierte Rollen (Sie als Verantwortlicher, der Tool-Anbieter als Auftragsverarbeiter)

Warum das wichtig ist: Ein AVV ist erforderlich, wenn ein Anbieter personenbezogene Daten in Ihrem Auftrag verarbeitet (Art. 28). Dies ist unabhängig von Ihrer Rechtsgrundlage nach Art. 6 für die Verarbeitung selbst – Sie brauchen beides. Einen Auftragsverarbeiter ohne Art. 28-konformen Vertrag einzusetzen, ist nicht konform, unabhängig von Ihrer Rechtsgrundlage.

Internationale Datenübertragungen

Wenn Ihr Tool-Anbieter außerhalb der EU ansässig ist (die meisten sind in den USA), benötigen Sie zusätzliche Schutzmaßnahmen:

Worauf Sie achten sollten:

• EU-Standardvertragsklauseln (SCCs), die in den Vertrag integriert sind

• Eine Transfer Impact Assessment (TIA), die die Rechtslage im Zielland und eventuelle ergänzende Maßnahmen dokumentiert

• Klare Informationen darüber, welche Unterauftragsverarbeiter Ihre Daten wo verarbeiten

• Die Option für echte EU-Datenresidenz (/post/eu-data-residency/) — Ihre Gesprächsdaten werden auf Infrastruktur gespeichert, die sich physisch in der Europäischen Union befindet

Warum das wichtig ist: Das Schrems-II-Urteil hat den EU-US Privacy Shield für ungültig erklärt. Tools, die Daten in die USA übertragen, stützen sich in der Regel auf SCCs, aber diese erfordern eine Einzelfallbewertung und bei Bedarf ergänzende Maßnahmen zur Gewährleistung eines angemessenen Schutzes.

Technische und organisatorische Maßnahmen (TOMs)

Worauf Sie achten sollten:

• Dokumentation der Sicherheitsmaßnahmen (Verschlüsselung, Zugriffskontrollen etc.)

• Informationen darüber, wo und wie Daten gespeichert werden

• Richtlinien zur Datenaufbewahrung – wie lange werden Daten gespeichert?

• Optionen für lokale/On-Device-Verarbeitung vs. Cloud-Verarbeitung

Warum das wichtig ist: Sie müssen überprüfen, dass Ihr Auftragsverarbeiter angemessene Sicherheitsmaßnahmen für die Sensibilität der von Ihnen verarbeiteten Daten hat.

KI-spezifische Aspekte

Worauf Sie achten sollten:

• Bestätigung, dass Ihre Daten nicht zum Training von KI-Modellen verwendet werden
• Klare Richtlinien zur Datenaufbewahrung bei KI-Unterauftragsverarbeitern (idealerweise Zero Retention)
• Transparenz darüber, welche KI-Dienste Ihre Daten verarbeiten

Warum das wichtig ist: Viele KI-Tools senden Gesprächsdaten an KI-Drittdienste. Sie brauchen Transparenz darüber, wer Ihre Daten verarbeitet und zu welchen Bedingungen. Obwohl die DSGVO keine spezifischen Aufbewahrungsfristen vorschreibt, begünstigen Datenminimierungsprinzipien kürzere Aufbewahrung, und Zero-Retention-Zusagen von KI-Unterauftragsverarbeitern reduzieren Ihr Risiko.

Unterauftragsverarbeiter-Transparenz

Worauf Sie achten sollten:

• Eine vollständige Liste der Unterauftragsverarbeiter mit deren Zwecken und Standorten
• Benachrichtigungsprozess bei Änderungen der Unterauftragsverarbeiter
• Möglichkeit, neuen Unterauftragsverarbeitern zu widersprechen

Warum das wichtig ist: Art. 28 Abs. 2 erfordert, dass Auftragsverarbeiter die Genehmigung des Verantwortlichen für Unterauftragsverarbeiter einholen. Sie brauchen Transparenz über jeden, der Ihre Daten berührt, und die Möglichkeit zu bewerten, ob deren Einbeziehung angemessen ist.

Teil 2: Ihre Pflichten als Verantwortlicher

Selbst mit einem vollständig konformen Tool haben Sie Pflichten, die keine Software für Sie erfüllen kann:

Bevor Sie mit der Aufzeichnung beginnen

Rechtsgrundlage

• Identifizieren Sie Ihre Rechtsgrundlage für die Verarbeitung nach Art. 6 DSGVO (berechtigtes Interesse, Einwilligung, Vertragserfüllung etc.)
• Dokumentieren Sie diese Grundlage und seien Sie bereit, sie auf Nachfrage zu erklären
• Hinweis: Einwilligung ist eine Option, aber berechtigte Interessen oder Vertragserfüllung können je nach Kontext angemessen sein

Transparenz und Informationspflicht

• Informieren Sie alle Meeting-Teilnehmer, dass KI-Tools das Gespräch verarbeiten werden
• Erklären Sie, was erfasst wird, wie es verarbeitet wird und wer Zugang hat
• Stellen Sie diese Informationen klar und vor Beginn der Verarbeitung bereit
• Praktische Vorlagen, die sowohl die DSGVO-Transparenz als auch die meisten lokalen Aufzeichnungsgesetze erfüllen, finden Sie in Erlaubnis zur Meeting-Aufnahme einholen (/post/ask-permission-to-record-meeting-consent-scripts/)

Aufzeichnungsgesetze (unabhängig von der DSGVO)

• Prüfen Sie lokale Gesetze zur Aufzeichnung von Gesprächen – viele Rechtsordnungen erfordern unabhängig von der DSGVO die Einwilligung der Teilnehmer
• Diese Anforderungen variieren je nach Land und können strenger sein als die DSGVO selbst

• Im Zweifelsfall deckt die Einholung einer ausdrücklichen Einwilligung sowohl die DSGVO-Transparenzanforderungen als auch die meisten lokalen Aufzeichnungsgesetze ab

Risikobewertung

• Prüfen Sie, ob eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist

• DSFAs sind bei Verarbeitungen vorgeschrieben, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von Personen mit sich bringen

• Faktoren, die auf ein hohes Risiko hinweisen können: umfangreiche Verarbeitung, sensible Daten, neue Technologien und systematische Überwachung

• Auch wenn nicht strikt erforderlich, sind DSFAs bei KI-basierter Verarbeitung eine gute Praxis und helfen, die Rechenschaftspflicht zu demonstrieren

Laufende Compliance

Datenschutzrichtlinien-Updates

• Aktualisieren Sie Ihre Datenschutzrichtlinie, um den Einsatz von KI-Meeting-Tools widerzuspiegeln

• Enthalten sollten: welche Daten erhoben werden, Zwecke, Rechtsgrundlage, Aufbewahrungsfristen, beteiligte Dritte und Betroffenenrechte

Betroffenenrechte

• Etablieren Sie Prozesse zur Bearbeitung von Auskunftsersuchen (Personen können fragen, welche Daten Sie über sie speichern)

• Ermöglichen Sie Löschanträge – Sie müssen in der Lage sein, die Daten einer Person aus Ihren Meeting-Aufzeichnungen zu entfernen

• Dokumentieren Sie, wie Sie Widersprüche bearbeiten, insbesondere wenn Sie sich auf berechtigte Interessen stützen

Aufbewahrung und Löschung

• Definieren Sie, wie lange Sie Meeting-Daten basierend auf Ihren angegebenen Zwecken aufbewahren

• Implementieren Sie regelmäßige Löschzeitpläne

• Datenminimierungsprinzipien bedeuten, dass Sie Daten nicht länger als nötig aufbewahren sollten

Dokumentation

• Führen Sie ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30

• Dokumentieren Sie Ihre Compliance-Maßnahmen und Entscheidungen

Jährliche Überprüfung

DSGVO-Compliance ist keine einmalige Aufgabe:

• Überprüfen Sie die aktualisierten Bedingungen, den AVV und die Unterauftragsverarbeiter-Liste Ihres Tools mindestens jährlich

• Bewerten Sie Ihre Rechtsgrundlage neu, wenn sich Ihre Anwendungsfälle ändern

• Aktualisieren Sie Ihre DSFA, wenn sich die Verarbeitungsaktivitäten wesentlich ändern

• Überprüfen Sie, ob Ihre Aufbewahrungszeitpläne eingehalten werden

Teil 3: Konfigurationsentscheidungen

Die meisten KI-Meeting-Tools bieten verschiedene Funktionen, die Ihre Datenschutzposition beeinflussen. Berücksichtigen Sie für jede aktivierte Funktion die Compliance-Auswirkungen. (Für Hedy-spezifische Konfigurationshinweise – was jede Einstellung bewirkt und welche empfohlenen Profile für Anwälte, Gesundheitsdienstleister und Coaches gelten – siehe Hedy Datenschutzeinstellungen erklärt (/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; }

Funktion	Datenschutzaspekt
Cloud Sync	Daten verlassen Ihr Gerät und werden auf den Servern des Anbieters gespeichert
Live-KI-Coaching/Vorschläge	Echtzeit-Datenübertragung an KI-Dienste
E-Mail-Zusammenfassungen	Meeting-Inhalte werden per E-Mail übertragen (in der Regel unverschlüsselt)
Audio-Aufzeichnungsspeicherung	Sprachaufnahmen sind personenbezogene Daten; siehe Hinweis unten zu biometrischen Daten
Teilen/Zusammenarbeit	Erweitert den Datenzugang auf weitere Parteien
API-Integrationen	Datenflüsse zu zusätzlichen Drittanbietersystemen

Hinweis zu Audioaufnahmen: Sprachaufnahmen sind personenbezogene Daten. Sie können unter Art. 9 als besondere Kategorien biometrischer Daten gelten, wenn sie zum Zweck der eindeutigen Identifizierung einer Person verarbeitet werden (z.B. Stimmabdruck-Analyse, Sprecheridentifikationssysteme). Standard-Meeting-Aufnahmen, die für Transkription und Notizerstellung verwendet werden, fallen in der Regel nicht in diese Kategorie, aber wenn Sie Stimmidentifikationsfunktionen nutzen, gelten die Anforderungen von Art. 9.

Allgemeines Prinzip: Aktivieren Sie nur, was Sie brauchen. Jede zusätzliche Funktion erweitert Ihren Datenverarbeitungsumfang und erfordert eine Rechtfertigung unter Datenminimierungsprinzipien.

Besondere Kategorien personenbezogener Daten

Wenn Ihre Meetings sensible Daten nach Art. 9 DSGVO betreffen – Gesundheitsinformationen, politische Meinungen, religiöse Überzeugungen, zur eindeutigen biometrischen Identifizierung verarbeitete Daten etc. – benötigen Sie verstärkte Schutzmaßnahmen:

• Eine spezifische Rechtsgrundlage sowohl nach Art. 6 ALS AUCH eine Bedingung nach Art. 9 Abs. 2
• Ausdrückliche Einwilligung wird häufig verwendet, aber andere Bedingungen können je nach Kontext gelten
• Stärkere Sicherheitsmaßnahmen entsprechend der Sensibilität
• DSFA wahrscheinlich erforderlich
• Überlegen Sie, ob Cloud-Funktionen angesichts des Risikoprofils angemessen sind

Teil 4: Praktische Umsetzung

Beispieltext für Hinweis und Einwilligung

Vor dem Start jedes aufgezeichneten Meetings:

> *„Ich möchte einen KI-Assistenten nutzen, um Notizen und Erkenntnisse aus unserem Gespräch festzuhalten. Das bedeutet, dass unsere Diskussion transkribiert und von KI analysiert wird. Das Transkript bleibt unter meiner Kontrolle und wird nicht zum Training von KI-Modellen verwendet. Sind Sie damit einverstanden?"*

Warten Sie auf die Bestätigung, bevor Sie starten. Dieser Ansatz erfüllt sowohl die DSGVO-Transparenzanforderungen als auch die meisten lokalen Aufzeichnungs-Einwilligungsgesetze.

Ergänzung in der Kalendereinladung

„Dieses Meeting wird durch KI-gestützte Notizerstellung unterstützt. Falls Sie Bedenken haben, teilen Sie mir das bitte vor dem Meeting mit."

Hinweis: Dies bietet eine Vorabinformation, was eine gute Praxis ist. Abhängig von Ihrer Rechtsgrundlage und lokalen Aufzeichnungsgesetzen müssen Sie möglicherweise zu Beginn des Meetings noch die Einwilligung bestätigen.

Datenschutzrichtlinien-Text (Vorlage)

Nehmen Sie in Ihre Datenschutzrichtlinie auf:

KI-gestützte Meeting-Unterstützung Wir nutzen KI-gestützte Tools zur Transkription und Analyse von Meetings zum Zweck der [Erfassung von Aufgaben / Verbesserung der Kommunikation / Führung genauer Aufzeichnungen]. Diese Verarbeitung basiert auf [Ihre Rechtsgrundlage, z.B. berechtigten Interessen an der Führung genauer Geschäftsaufzeichnungen / Vertragserfüllung / Einwilligung]. Meeting-Daten können von unserem KI-Meeting-Tool-Anbieter und deren Unterauftragsverarbeitern verarbeitet werden. Daten können unter EU-Standardvertragsklauseln mit geeigneten ergänzenden Maßnahmen in die USA übertragen werden. Meeting-Transkripte und -Zusammenfassungen werden für [X Zeitraum] aufbewahrt und dann gelöscht. Sie können Auskunft, Berichtigung oder Löschung Ihrer Daten unter [Kontaktdaten] beantragen.

Passen Sie dies an Ihre spezifische Situation und Rechtsgrundlage an.

Wie Hedy DSGVO-Compliance handhabt

Wir haben Hedy mit Datenschutz als Kernprinzip entwickelt, nicht als Nachgedanken. Für die vollständige Aufschlüsselung der DSGVO-Konformität von Hedy (/post/hedy-ai-gdpr-compliance/) — einschließlich AVV, SCCs und Transfer Impact Assessment — lesen Sie den dedizierten Beitrag. So haben wir die Anforderungen dieser Checkliste adressiert:

Vertragliches Framework

• Auftragsverarbeitungsvertrag mit EU-Standardvertragsklauseln automatisch in Ihrem Konto enthalten

• Transfer Impact Assessment mit Dokumentation der Schutzmaßnahmen für US-Datenübertragung und ergänzende Maßnahmen verfügbar

• Vollständige Dokumentation technischer und organisatorischer Maßnahmen

• Transparente Unterauftragsverarbeiter-Liste mit Änderungsbenachrichtigungen

Privacy-First-Architektur

• On-Device-Spracherkennung standardmäßig – Ihr Audio verlässt nie Ihr Gerät, sofern Sie keine Cloud-Funktionen aktivieren

• Zero-Retention-Vereinbarungen mit KI-Unterauftragsverarbeitern

• Ihre Daten werden nie zum Training von KI-Modellen verwendet

• Granulare Kontrollen: Aktivieren Sie nur die Funktionen, die Sie brauchen

Compliance-Dokumentation

• Vollständige Dokumentation in unserem Trust Center verfügbar

• DSGVO-Compliance-Leitfaden für Nutzer (Pflichten als Verantwortlicher)
• SOC 2 Type I- und HIPAA-Zertifizierungen in Bearbeitung (erwartet Q2 2026)

Nutzerkontrolle

• Reiner Offline-Modus für maximalen Datenschutz verfügbar
• Löschen Sie Ihre Daten jederzeit
• Exportieren Sie Ihre Daten für die Datenportabilität
• EU-Datenschutzregion-Einstellung zur Minimierung von Tracking

Greifen Sie auf unsere vollständige Compliance-Dokumentation unter trust.hedy.ai (https://trust.hedy.ai) zu.

Häufig gestellte Fragen

Wie bewerte ich ein KI-Meeting-Tool auf DSGVO-Konformität?

Prüfen Sie vier Dinge: einen AVV, der Art. 28 erfüllt (mit EU-SCCs, wenn der Anbieter außerhalb der EU sitzt), eine Transfer Impact Assessment, die US-Datenschutzgesetze und ergänzende Maßnahmen dokumentiert, dokumentierte technische/organisatorische Maßnahmen und eine vollständige Unterauftragsverarbeiter-Liste mit Benachrichtigungsrechten. Wenn ein Anbieter nicht alle vier vorlegen kann, ist er für Ihr Unternehmen nicht DSGVO-bereit.

Welche Fragen sollte ich einem Anbieter zur DSGVO stellen?

Fünf Basisfragen: (1) Können Sie einen AVV mit Art.-28-Klauseln bereitstellen? (2) Wo werden Daten physisch gespeichert, und bieten Sie EU-Residenz an? (3) Sind EU-Standardvertragsklauseln für alle Nicht-EU-Übermittlungen einbezogen, und ist eine TIA verfügbar? (4) Wer sind Ihre Unterauftragsverarbeiter und wo arbeiten sie? (5) Werden meine Daten jemals zum Training von KI-Modellen verwendet? Wenn eine Antwort fehlt, haken Sie nach.

Was ist eine Standardvertragsklausel und brauche ich eine?

Standardvertragsklauseln (SCCs) sind von der EU genehmigte Vertragsvorlagen, die einen Datenimporteur außerhalb der EU an EU-Schutzniveau binden, wenn personenbezogene Daten aus der EU übermittelt werden. Nach Schrems II stützen sich US-basierte Anbieter typischerweise auf SCCs plus ergänzende Maßnahmen, die in einer Transfer Impact Assessment dokumentiert sind. Wenn Ihr Anbieter in den USA sitzt und personenbezogene EU-Daten verarbeitet, ja — Sie brauchen SCCs.

Brauche ich eine Datenschutz-Folgenabschätzung für KI-Meeting-Tools?

Eine DSFA ist nach Art. 35 verpflichtend, wenn die Verarbeitung voraussichtlich ein hohes Risiko für betroffene Personen mit sich bringt — typische Auslöser sind systematische Überwachung, umfangreiche Verarbeitung, sensible Daten oder neue Technologien. KI-basierte Aufzeichnung erfüllt oft einen oder mehrere Auslöser. Selbst wenn sie nicht zwingend erforderlich ist, ist eine DSFA gute Praxis und demonstriert Rechenschaftspflicht.

Welche Pflichten habe ich als Verantwortlicher beim Einsatz von KI-Meeting-Tools?

Legen Sie eine Rechtsgrundlage nach Art. 6 fest (berechtigtes Interesse, Einwilligung, Vertragserfüllung), informieren Sie Teilnehmende vor der Aufzeichnung transparent, führen Sie ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30, erstellen Sie eine DSFA wo erforderlich, bearbeiten Sie Betroffenenrechte (Auskunft, Löschung, Widerspruch) und aktualisieren Sie Ihre Datenschutzrichtlinie. Der Anbieter erfüllt auftragsverarbeiterseitige Pflichten; Sie erfüllen die Pflichten des Verantwortlichen.

Fragen?

DSGVO-Compliance kann komplex erscheinen, muss aber nicht überwältigend sein. Wenn Sie Fragen zur DSGVO-konformen Nutzung von Hedy haben, kontaktieren Sie uns unter privacy@hedy.ai (mailto:privacy@hedy.ai) oder konsultieren Sie unsere Hilfe-Dokumentation (https://help.hedy.bot) .

Für komplexe Compliance-Fragen, die spezifisch für Ihre Organisation sind, empfehlen wir die Beratung durch einen qualifizierten Datenschutzexperten oder Ihren Datenschutzbeauftragten.

Dieser Leitfaden bietet allgemeine Informationen zur DSGVO-Compliance für KI-Meeting-Tools. Er stellt keine Rechtsberatung dar und sollte nicht als solche herangezogen werden. Die Anforderungen können je nach Ihrer spezifischen Situation, Rechtsordnung und der Art der von Ihnen verarbeiteten Daten variieren. Lokale Gesetze zur Aufzeichnung von Gesprächen können zusätzliche Anforderungen über die DSGVO hinaus auferlegen.
