Wie privat ist Ihr KI-Notiztool?

KI-Notiztools machen aus Ihrem Meeting eine Aufzeichnung, die jemand anderes verwahrt. Erfahren Sie, was bei jedem Schritt das Gerät verlässt, wie Sie die Aussagen eines Tools prüfen und wie alles lokal bleibt.

Veröffentlicht von Julian Pscheid · 15. Juli 2026 · Aktualisiert 20. August 2026
Diesen Artikel online lesen: https://www.hedy.ai/de/post/how-to-use-ai-meeting-notes-privately/

Zwei Kolleginnen und Kollegen im Gespräch an einem kleinen Tisch in einem privaten Büro mit geschlossener Tür, zwischen ihnen ein mit dem Display nach unten liegendes iPhone neben einem Notizbuch und einer entenförmigen Kaffeetasse der Oregon Ducks

Kurzantwort Ein KI-Notiztool für Meetings erledigt drei Aufgaben, bei denen jeweils Daten abfließen können: Es transkribiert Ihr Audio, analysiert das Transkript und speichert das Ergebnis. Die meisten Tools führen alle drei Schritte auf ihren eigenen Servern aus. So wird das Meeting zu einer durchsuchbaren Aufzeichnung, die jemand anderes verwahrt. Einige wenige können alle drei Schritte auf Ihrer eigenen Hardware ausführen. Nur bei dieser Konfiguration verlassen keine Daten über das Meeting den Raum. Hedy transkribiert standardmäßig auf jeder unterstützten Plattform auf dem Gerät. Auf den meisten aktuellen Geräten kann auch die Analyse lokal laufen. Ist zusätzlich Hedys Cloud Sync deaktiviert, gelangt nichts aus dem Gespräch auf unsere Server, es sei denn, Sie teilen diese Sitzung ausdrücklich.

The Associated Press veröffentlichte diesen Monat einen Beitrag über KI-Notiztools am Arbeitsplatz, der die Risiken gut zusammenfasst (AP, Juli 2026 (https://apnews.com/article/ai-notetaker-work-meetings-privacy-data-c700299371ca7cfec77dafdfb948067f)): vertrauliche Personaldaten, Unternehmensstrategie, Geschäftsgeheimnisse und Äußerungen, die in einer späteren Vernehmung schlecht aussehen. Auch die Ratschläge sind sinnvoll. Prüfen Sie, ob ein Notiztool beigetreten ist. Holen Sie vor einem sensiblen Meeting die Einwilligung ein. Stützen Sie sich auf Unternehmensrichtlinien,

damit nicht eine einzelne Person widersprechen muss. Schalten Sie das Tool für den heiklen Teil aus. Fragen Sie, was der Anbieter speichert und ob er mit etwas davon trainiert.

Jede dieser Maßnahmen begrenzt die Folgen, wenn Ihr Meeting zu einer Aufzeichnung in fremder Hand wird. Keine stellt die Frage, ob das überhaupt nötig ist. Justin Daniels, Unternehmensanwalt bei Baker Donelson, brachte es in dem Beitrag am treffendsten auf den Punkt: „Ich spreche über nichts Substanzielles, bevor das Tool abgeschaltet ist, denn ich möchte dieses Risiko schlicht nicht eingehen.“ Für die Tools, die die meisten Menschen nutzen, ist das der richtige Rat. Er setzt voraus, dass das Meeting Ihre Hardware verlassen muss.

Auf aktuellen Geräten muss es das nicht. Einige wenige Produkte können die gesamte Pipeline auf Ihrem eigenen Gerät ausführen, und fast niemand weiß davon.

Was verlässt Ihr Gerät, wenn Sie ein Notiztool verwenden?

Drei Dinge, und bei jedem können unabhängig Daten abfließen. Die Transkription verwandelt Ihr Audio in Text. Die Analyse liest diesen Text und erstellt Ihre Zusammenfassung und Aufgaben. Die Speicherung entscheidet, ob etwas davon dauerhaft an einem Ort verbleibt, den Sie nicht kontrollieren. Jeder Schritt kann auf Ihrer eigenen Hardware bleiben oder auf die eines anderen wechseln. Daraus ergeben sich acht mögliche Kombinationen.

Schritt	Funktion	Kann auf dem Gerät laufen?	Was das Gerät andernfalls verlässt
Transkription	Wandelt Audio in Text um, teilweise mit Sprecherlabels	Ja, auf aktueller Hardware	Das Audio selbst und bei vielen Systemen zusätzlich ein akustisches Embedding pro Person
Analyse	Liest das Transkript und erstellt Zusammenfassungen und Aufgaben	Ja, auf leistungsfähiger Hardware	Das Transkript und alles, was ein Modell daraus ableitet
Speicherung und Synchronisierung	Bewahrt das Archiv auf	Ja, wenn sie deaktiviert bleibt	Eine dauerhafte, durchsuchbare Kopie sowie Metadaten, die auch nach dem Löschen fortbestehen können

Hier verstecken sich die meisten Datenschutzaussagen. „Audiodaten verlassen Ihr Gerät nie“ klingt wie eine Aussage über das gesamte Produkt. Sie bedeutet nur, dass die Transkription lokal stattfindet. Das ist durchaus damit vereinbar, das vollständige wortgetreue Transkript eine Sekunde später an ein Sprachmodell zu senden. Hedy tut standardmäßig genau das. Deshalb ist „Verlässt das Audio das Gerät?“ die falsche Stelle, um mit den Fragen aufzuhören. Das Transkript ist die Aufzeichnung. Sobald es Ihr Gerät verlässt, hat auch fast alles, worüber Sie sich beim Audio Sorgen gemacht haben, Ihr Gerät verlassen.

Hybride Verarbeitung ist üblich, auch bei Hedys Standardeinstellung. Problematisch ist ein Anbieter, der nicht sagt, welche Schritte Ihr Gerät verlassen.

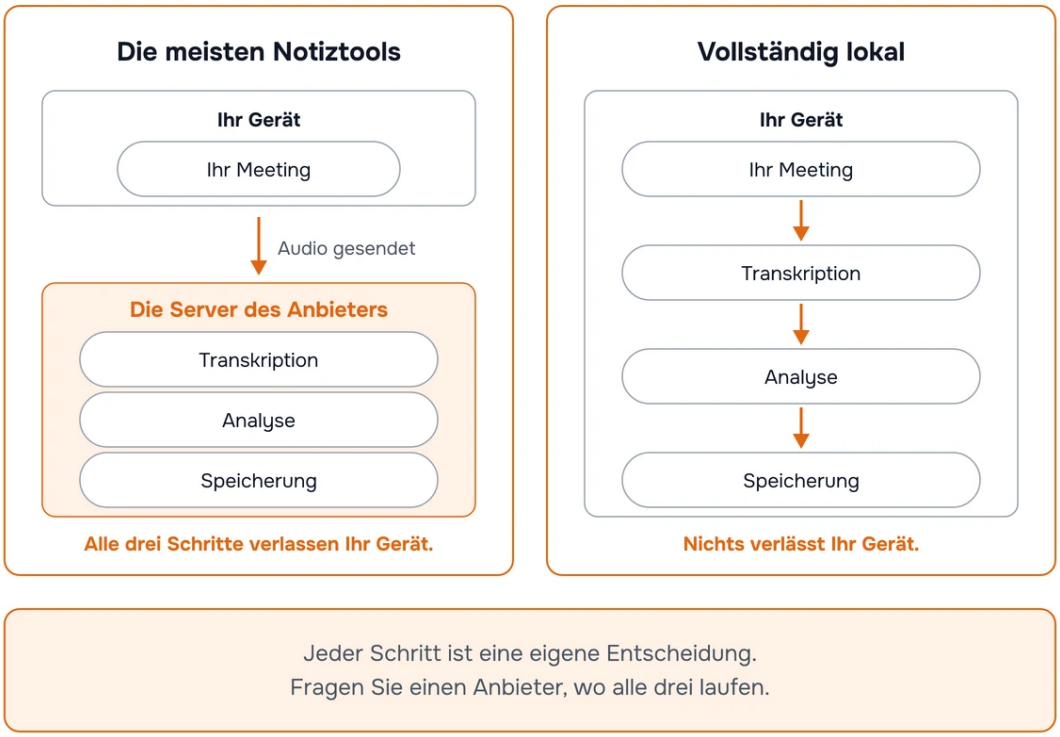

Diagramm zum Vergleich der meisten Notiztools, bei denen das Audio an die Server des Anbieters gesendet wird und Transkription, Analyse und Speicherung dort stattfinden, mit einer vollständig lokalen Konfiguration, bei der alle drei Schritte auf Ihrem eigenen Gerät stattfinden

Kann die gesamte Pipeline auf Ihrem Gerät laufen?

Ja, auf aktueller Hardware. Genau das hat sich unbemerkt verändert. Nur sehr wenige Produkte führen alle drei Schritte lokal aus.

Die Transkription ist der einfachere Schritt

Whisper, die Standard-Engine, läuft auf jeder Plattform, auf der Hedy angeboten wird. Nemotron läuft auf jeder nativen Plattform, aber nicht in der Web-App. Nemotron ist eine Streaming-Engine auf Basis von NVIDIAs Sprachmodell mit 600 Millionen Parametern (https://huggingface.co/nvidia/nemotron-3.5-asr-streaming-0.6b) . Sie ergänzt die Sprecherlabels, für die früher häufig eine Cloud-Engine nötig war. Erforderlich sind ein einmaliger Download von ungefähr 0,6 bis 0,7 GB und Hardware ab etwa der iPhone-12-Generation. Die Genauigkeit hängt weiterhin von Akzent, Raumgeräuschen, gleichzeitigem Sprechen und Fachvokabular ab. Testen Sie die Engine deshalb in Ihren eigenen Meetings, statt sich auf veröffentlichte Werte zu verlassen.

Bei der Analyse liegt der Kompromiss

Local AI Processing (/de/help/local-ai-processing/) erstellt Zusammenfassungen und Vorschläge auf Ihrem Gerät und benötigt dafür leistungsfähige Hardware: einen Apple Silicon Mac, einen Windows-PC mit geeigneter GPU oder ein aktuelles iPhone oder iPad. Die Modelle reichen von etwa 1,2 GB für die mobile Stufe bis zu mehr als 20 GB. Ein Modell der mittleren Stufe mit ungefähr 9 Milliarden Parametern läuft auf einem Mac mit 16 GB komfortabel. Die größten Modelle benötigen ungefähr 25 GB RAM oder mehr.

Local AI Processing ist standardmäßig deaktiviert, weil die Cloud-Analyse schneller ist und derzeit bessere Ergebnisse liefert. Hedys Standardeinstellung ist bewusst aufgeteilt: Die Spracherkennung läuft überall lokal, damit das Audio nie ohne Ihre ausdrückliche Entscheidung das Gerät verlässt. Die Analyse findet in der Cloud statt, damit das Produkt auf Hardware gut funktioniert, die kein Sprachmodell ausführen kann. Eine Zusammenfassung, die in der Cloud sofort erscheint, kann lokal zwischen dreißig Sekunden und mehreren Minuten benötigen. Die technische Analyse (/de/post/local-ai-engineering-deep-dive-hedy-3-2/) enthält die vollständige Aufschlüsselung.

Local AI Processing fällt nicht unbemerkt auf die Cloud zurück. Wenn lokal etwas fehlschlägt, erhalten Sie eine Fehlermeldung statt eines stillen neuen Versuchs auf einem Server. Ein stiller Rückfall ist die schlechteste Eigenschaft, die eine Datenschutzfunktion haben kann. Sie versagt genau in die Richtung, die Sie verhindern wollten, und informiert Sie nicht darüber.

Speicherung ist ein Schalter, keine Funktion

Der oft vergessene Schritt ist das Archiv, denn es erscheint als Komfortfunktion. Cloud Sync kopiert Sitzungsdaten auf Hedys Server, damit Ihre anderen Geräte darauf zugreifen können. Bleibt Cloud Sync aktiviert, erhalten Sie geräteübergreifenden Zugriff bei lokaler Verarbeitung. Deaktivieren Sie die Funktion, und nichts aus dem Gespräch gelangt auf unsere Server, es sei denn, Sie teilen diese Sitzung ausdrücklich. Lokale Verarbeitung und lokale Speicherung sind getrennte Entscheidungen. Ein Tool, das nur die erste anbietet, hat die Pipeline nicht vollständig geschlossen.

Wie prüfen Sie die Aussagen eines Notiztools?

Beobachten Sie das Verhalten und lesen Sie dann die Dokumentation. Keines von beidem reicht allein aus.

Probieren Sie den Flugmodus aus. Deaktivieren Sie alle Netzwerkverbindungen und starten Sie eine Sitzung. Wenn ein Tool weiter transkribiert und zusammenfasst, existiert ein lokaler Weg. Das ist eine nützliche Erkenntnis, aber kein Beweis. Bleibt das Tool stehen, könnte es eine Anmeldung oder einen Modell-Download verlangen, statt die Cloud zu benötigen. Und ein Tool mit funktionierendem Offline-Weg kann alles über einen Server leiten, sobald Sie die Verbindung wiederherstellen. Der Test zeigt, dass ein lokaler Modus existiert. Er verrät nicht, was im Onlinebetrieb passiert.

Achten Sie auf die Frage nach Sprecherlabels. Wenn ein Tool Sprecherlabels anzeigt und behauptet, nichts verlasse Ihr Gerät, fragen Sie, welche On-Device-Engine die Sprechertrennung übernimmt. Kann ein Anbieter die Engine benennen, liefert er eine konkrete Information. Kann er es nicht, erfolgt die Zuordnung möglicherweise auf einem Server.

Lesen Sie die Unterauftragsverarbeiter-Liste. Eine Datenschutzrichtlinie soll beruhigen. Die Unterauftragsverarbeiter-Liste dient der Beschaffung und vertraglichen Information. Deshalb nennt sie die Unternehmen im Datenfluss. Hedys Liste umfasst unter trust.hedy.ai (https://trust.hedy.ai) sechzehn Einträge. Prüfen Sie bei jedem Anbieter, welche Unternehmen Meeting-Inhalte erhalten können und aus welchem Grund. Die Länge der Liste allein sagt wenig aus.

Fragen Sie, was nach dem Löschen erhalten bleibt. Danielle Kays, Partnerin bei Fisher Phillips, wies darauf hin, dass Meeting-Metadaten nach dem Löschen von Inhalten beim Anbieter verbleiben können. Aufgenommene Inhalte können in manchen Fällen zudem von einem Modell memorisiert oder reproduziert werden. Die Bedeutung von „löschen“ unterscheidet sich je nach Anbieter. Häufig heißt es nur, etwas aus der für Sie sichtbaren Ansicht zu entfernen.

Wenn es wirklich darauf ankommt, prüfen Sie den Datenverkehr. Offline-Tests und Datenschutzseiten beantworten unterschiedliche Fragen, und keines von beidem beobachtet das Netzwerk. Bei einem regulierten Einsatz ist eine Paket- oder DNS-Analyse die Prüfung, die tatsächlich zeigt, was ein Tool sendet.

Was sollten Sie vor der Installation fragen?

Fünf Fragen. Jede Antwort sollte konkret sein.

1. Wo läuft jeder der drei Schritte? Transkription, Analyse und Speicherung müssen einzeln benannt werden. Fragen Sie nicht bloß, ob das Tool „privat“ ist.
2. Erstellen Sie Sprecherlabels, und wo? Erfolgt dies auf einem Server, fragen Sie, was das Embedding enthält, wie lange es gespeichert wird und welche Information die Teilnehmenden erhalten.
3. Wie sehen die Aufbewahrungs- und Löschfristen aus? Verlangen Sie eine schriftliche Frist. Illinois fordert genau das. Den später zitierten Juristinnen und Juristen zufolge verfügen die meisten Unternehmen, die solche Tools einsetzen, nicht darüber.
4. Wer sind die Unterauftragsverarbeiter, und wo arbeiten sie? Bei europäischen Teilnehmenden ist das zugleich die DSGVO-Frage (/de/post/gdpr-checklist-ai-meeting-tools/) . Jüngste Entwicklungen bei EU-US-Datenübermittlungen (/de/post/eu-us-data-transfers-supreme-court-ftc-ruling/) haben deren Rechtsgrundlage weniger verlässlich gemacht als zuvor.
5. Wechselt das Tool bei einem Fehler zur Cloud, und weist es darauf hin? Ein stiller Rückfall macht aus einer Datenschutzeinstellung bloße Dekoration.

Wie nutzen Sie Hedy, ohne dass etwas Ihr Gerät verlässt?

Prüfen Sie eine Standardeinstellung und ändern Sie anschließend zwei Einstellungen.

Öffnen Sie Settings !’ Speech & AI . Vergewissern Sie sich, dass Whisper oder Nemotron ausgewählt ist. Whisper ist bereits die Standardeinstellung. Die meisten Menschen müssen daher nichts ändern. Handeln müssen Sie nur, wenn jemand zu einem Cloud-Anbieter gewechselt hat.

Aktivieren Sie auf demselben Bildschirm Local AI Processing und wählen Sie ein Modell mit dem Label „Great fit“. Hedy prüft den verfügbaren Arbeitsspeicher und kennzeichnet jedes Modell als Great fit, Tight fit oder Won't fit. Sie müssen also nicht raten. Die Einstellung gilt pro Gerät. Auf Ihrem Mac und Ihrem iPhone müssen Sie sie jeweils separat vornehmen.

Deaktivieren Sie anschließend Cloud Sync . Ist die Funktion aus, gelangen keine Meeting-Daten auf unsere Server, es sei denn, Sie teilen eine Sitzung ausdrücklich.

Wenn Ihre Hardware kein lokales Modell ausführen kann, ist die Datenschutzeinstellung für Cloud-KI-Analyse (/de/help/cloud-ai-analysis-privacy-control/) der Mittelweg. Sie stoppt die Cloud-Analyse, während die lokale Transkription weiterläuft. So erhalten Sie ein privates Transkript ohne KI-generierte Notizen. Unsere Erklärung der Datenschutzeinstellungen (/de/post/ai-meeting-privacy-settings-explained/) beschreibt die vollständige Matrix, und die Sicherheitsseite (/de/security/) dokumentiert jede Konfiguration.

Benötigt ein privates Notiztool trotzdem die Einwilligung?

Ja. Ein gerätebasiertes Tool ist für andere Menschen schwerer zu erkennen als ein Bot.

AP wies darauf hin, dass Teilnehmende persönliche Notizgeräte verwenden können, die von der Meeting-Plattform getrennt sind, „sodass die anderen Beteiligten nicht unbedingt wissen, dass ein Gespräch aufgezeichnet und transkribiert wird“. Ein Bot erscheint in der Teilnehmendenliste. Eine App auf dem Telefon einer Person ist unsichtbar. Dadurch werden unbemerkte Aufnahmen leichter. Das ist eine berechtigte Kritik an der Kategorie, zu der auch wir gehören. Thorin Klosowski, leitender Analyst für Sicherheit und Datenschutz bei der Electronic Frontier Foundation, gab die klare Antwort: „Vor einem sensiblen Meeting alle um Einwilligung zu bitten, wäre die höflichste Vorgehensweise.“

Lokale Verarbeitung bestimmt, wohin Daten gelangen. Sie sagt nichts darüber aus, ob jemand zugestimmt hat. Aufnahmerecht, Arbeitsplatzrichtlinien und berufliche Pflichten gelten unabhängig von der Architektur weiter. Wenn Sie ein Tool verwenden, das niemand sehen kann, steigt Ihre Pflicht, darauf hinzuweisen.

Ein Aspekt wird allerdings leichter: das Gespräch darüber. Der meiste Widerstand gegen eine Aufnahme richtet sich nicht gegen die Notizen, sondern gegen das Archiv: Wer kann es noch sehen? Wie lange bleibt es erhalten? Was passiert, wenn der Anbieter übernommen wird? „Es bleibt auf meinem Laptop und ich lösche es danach“ ist ein anderes Gespräch als „Es wird zu einem Dienst hochgeladen, dessen Bedingungen ich nicht gelesen habe.“ Für die unangenehme Situation haben wir wortgetreue Einwilligungsvorlagen (/de/post/ask-permission-to-record-meeting-consent-scripts/) erstellt. Unser Artikel über Gesetze zur Aufnahme von Gesprächen und Einwilligung (/de/help/recording-laws-and-consent/) behandelt die rechtliche Seite.

Chris Pluymers, Rechtsanwalt bei The Dillon Law Group, schlug zudem folgende Formulierung vor, um ein Notiztool abzulehnen: „Ich möchte dieses Meeting lieber ohne KI-Aufzeichnung oder Transkriptions-Tools durchführen. Ich mache gern eigene Notizen und teile anschließend eine Zusammenfassung, falls das hilfreich ist.“ Amy Dufrane, Geschäftsführerin des HR-Zertifizierungsverbands HRCI, empfahl, die Ablehnung institutionell statt persönlich zu begründen. Eine Unternehmensrichtlinie verhindert, dass eine einzelne Person widersprechen muss.

Warum sind Transkripte riskanter als Aufnahmen?

Klosowski formulierte im AP-Beitrag die treffendste Beobachtung: „Große Mengen Video zu speichern ist nicht einfach. Es ist teuer und schwer zu durchsuchen. Text lässt sich dagegen viel leichter durchsuchen und günstiger speichern.“

Vor KI-Notiztools bot die umständliche Nutzung einer Aufnahme einen praktischen Schutz. Ein zweistündiges Meeting ist ein zweistündiges Objekt. Ohne Anlass hört niemand es durch. Die Speicherkosten sind hoch genug, dass Aufnahmen gelöscht werden. Diese Hürde leistete echte Sicherheitsarbeit, ohne dass jemand dafür ein Budget einplanen musste.

Transkripte beseitigen sie. Text ist günstig genug, um ihn unbegrenzt aufzubewahren, und sofort nach dem Speichern durchsuchbar. Eine einzige Suche in vier Jahren Archiv findet jedes Vorkommen einer Formulierung für jede Person mit Zugriff, einschließlich der gegnerischen Rechtsvertretung mit einer Herausgabeanordnung. Eine Bemerkung, die in einer ungehörten Aufnahme verschwunden wäre, wird zum Suchergebnis.

Ganz eindeutig gefährlicher ist das Transkript allerdings nicht. Audio enthält Dinge, die Text verliert: Tonfall, Gespräche im Hintergrund und genug von Ihrer Stimme, um sie zu klonen. Audio kann außerdem später transkribiert werden. Eine Aufnahme ist also ein noch nicht erstelltes Transkript. Der Wandel führt von „Jemand könnte das finden“ zu „Jemand kann das sofort finden“. Die meisten Menschen haben diesen Unterschied nie einkalkuliert.

Was ist ein Stimmabdruck, und wer besitzt Ihren?

Pluymers beschrieb den Mechanismus: Um Person 1 von Person 2 zu unterscheiden, leiten viele Notiztools für jede Stimme eine akustische Signatur ab. Dieser Vorgang heißt Sprechertrennung oder Diarisierung. Diesen Zusammenhang dürften die meisten Leserinnen und Leser bisher nicht bedacht haben.

Die aktuelle Rechtslage

In Illinois gelten Stimmabdrücke nach dem Biometric Information Privacy Act als biometrische Identifikatoren. Das Gesetz verlangt eine schriftliche Information, die Offenlegung des Zwecks und der Aufbewahrungsdauer, eine unterzeichnete Freigabe vor der Erhebung und einen dokumentierten Löschplan (740 ILCS 14/15 (https://www.ilga.gov/ftp/ILCS/Ch%200740/Act%200014/074000140K15.html)). Ob ein Embedding zur Sprechertrennung als solcher Stimmabdruck gilt, ist eine neue, gerichtlich erprobte Theorie und noch keine geklärte Rechtslage (Lewis Rice (https://www.lewisrice.com/publications/ai-transcription-tools-give-rise-to-bipa-claims)). Manche durchgängigen Systeme zur Sprechertrennung funktionieren nicht einmal auf diese Weise. Sie ordnen Audio anonymen Sprecherindizes zu, ohne eine dauerhafte Vorlage zu erstellen.

Die Verfahren sind real. KI-Meeting-Tools sind ein aktuelles Ziel von BIPA-Sammelklagen (Fisher Phillips (https://www.fisherphillips.com/en/insights/insights/ai-meeting-tools-are-the-latest-target-of-illinois-bipa-class-actions)). Fireflies.ai ist Beklagte in einer angestrebten Sammelklage. Darin wird behauptet, der Dienst zeichne die Stimmen von Teilnehmenden auf, transkribiere und speichere sie, darunter auch Personen ohne eigenes Konto, und biete nicht die vorgeschriebene Information, Einwilligung und Absicherung der Aufbewahrung (Jackson Lewis (https://www.workplaceprivacyreport.com/2026/04/articles/artificial-intelligence/ai-meeting-assistants-and-biometric-privacy-governance-lessons-from-the-fireflies-ai-lawsuit/)). Das sind Behauptungen. Ein Gericht hat noch nicht in der Sache entschieden.

Was ein gestohlener Stimmabdruck kann und nicht kann

Die beängstigende Version ist weit verbreitet und sollte korrigiert werden: Ein gestohlenes Embedding zur Sprechertrennung ist kein Schlüssel zu Ihrem Bankkonto. Banken erfassen eigene Stimmvorlagen. Das interne Embedding eines Anbieters ist damit nicht austauschbar. Das tatsächliche Stimmrisiko ist gewöhnlicher und dennoch ernst genug: Ausreichend aufgezeichnetes Audio kann genügen, um eine Person überzeugend zu klonen (FTC (https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/04/approaches-address-ai-enabled-voice-cloning)). Das ist ein Argument über das Audio, nicht über das Embedding.

Wie Sprechertrennung auf dem Gerät das Risiko verändert

Für die Sprechertrennung auf dem Gerät gibt es einen nützlichen Präzedenzfall. In Barnett v. Apple bestätigte ein Berufungsgericht in Illinois die Abweisung einer BIPA-Sammelklage zu Face ID und Touch ID. Apple habe die biometrischen Daten der Nutzerinnen und Nutzer weder besessen noch erhoben, weil sie deren eigene Geräte nie verließen, nie an Apples Server gesendet wurden und die Funktionen freiwillig und löschbar waren (Duane Morris (https://blogs.duanemorris.com/classactiondefense/2023/01/09/illinois-appellate-court-affirms-dismissal-of-bipa-class-action-lawsuit/) , IAPP (https://iapp.org/news/b/court-rules-apples-facial-fingerprint-tools-comply-with-bipa)). Das lässt sich gut auf lokale Sprechertrennung übertragen: auf Ihrem Gerät abgeleitet, nie übertragen, optional und löschbar. Hedys Nemotron-Engine (/de/post/nemotron-on-device-speech-engine/) arbeitet auf diese Weise.

Das ist kein geschützter Freiraum. Barnett hing von den konkreten Umständen ab. Ein anderes Design oder ein anderer Klagevortrag könnte zu einem anderen Ergebnis führen. Zudem sagt der Fall nichts über die Pflichten der Person aus, die das Meeting einberufen hat. Es handelt sich um Risikominderung mit einem guten Präzedenzfall im Hintergrund, und nichts davon ist Rechtsberatung.

Kann ein Notiztool das Mandatsgeheimnis beeinträchtigen?

Ein Bundesgericht hat entschieden, dass KI-generierte Dokumente nicht privilegiert waren.

Die Entscheidung des Gerichts

In United States v. Heppner entschied Richter Jed Rakoff vom Southern District of New York im Februar 2026, dass Dokumente, die ein Angeklagter durch Eingabe von Informationen seiner Anwälte in einen Chatbot erzeugt hatte, weder dem Mandatsgeheimnis noch dem Schutz als anwaltliches Arbeitsergebnis unterlagen. Das Tool erstellte aus seinen Prompts 31 Dokumente, darunter eine Gliederung seiner eigenen Verteidigungsstrategie (Harvard Law Review (https://harvardlawreview.org/blog/2026/03/united-states-v-heppner/)). Rakoff nannte drei Gründe: Der Chatbot sei „offenkundig kein Anwalt“. Seine eigenen Hinweise warnten davor, die Ausgabe als Rechtsberatung zu betrachten, was die Behauptung entkräftete, Rechtsberatung sei der überwiegende Zweck gewesen. Außerdem wies die veröffentlichte Datenschutzrichtlinie des Anbieters darauf hin, dass Nutzerdaten in Gerichtsverfahren weitergegeben werden könnten. Der Nutzer konnte daher keine berechtigte Erwartung an Vertraulichkeit haben (Dorsey (https://www.dorsey.com/newsresources/publications/client-alerts/2026/2/ai-attorney-client-privilege)).

Dieser mittlere Punkt verdient einen zweiten Blick. Die Datenschutzrichtlinie war nicht die Verteidigung. Sie war das Beweismittel. Das Dokument, mit dem der Anbieter seine eigenen Datenpraktiken beschrieb, wurde zum Grund dafür, dass die Vertraulichkeitserwartung des Nutzers unangemessen war.

Wie weit die Entscheidung reicht

Heppner entschied nicht, ob ein Meeting-Notiztool zum Verlust des Mandatsgeheimnisses führt. Der Fall betraf einen Angeklagten, der auf eigene Initiative einen Chatbot nutzte, und kein Tool, das einem vertraulichen Gespräch beiwohnte. Kommentatorinnen und Kommentatoren arbeiten noch heraus, was er für Notiztools bedeutet (Columbia Blue Sky (https://clsbluesky.law.columbia.edu/2026/06/16/cahill-discusses-a-i-note-takers-in-corporate-meetings/)). The New York City Bar veröffentlichte eine formelle Stellungnahme zu den ethischen Fragen bei KI-Aufzeichnung und -Transkription von Mandantengesprächen, die Aufzeichnung und Aufbewahrung als getrennte Probleme behandelt (NYC Bar Formal Op. 2025-6 (https://www.nycbar.org/reports/formal-opinion-2025-6-ethical-issues-affecting-use-of-ai-to-record-transcribe-and-summarize-conversations-with-clients/)).

Die engere Warnung gilt trotzdem: Wenn Sie vertrauliches Material an einen Dritten senden, kann das die Erwartung schwächen, dass es vertraulich bleibt. Bei einer Pipeline ohne Dritte stellt sich diese Frage nicht. Sie begründet aber auch kein Mandatsgeheimnis, verhindert keine Herausgabe im Verfahren und macht ein unzulässig aufgezeichnetes Gespräch nicht zulässig. Daniels formulierte die praktische Seite klar: „Wenn die Daten an irgendeine andere Stelle gehen und die Beteiligten nichts davon wissen, ist dieses Gespräch möglicherweise nicht mehr vom Mandatsgeheimnis geschützt.“

Welche Meetings benötigen eine vollständig lokale Konfiguration?

Nicht alle. Etwas anderes zu behaupten würde den Rat leicht angreifbar machen.

Für ein wöchentliches Statusmeeting ist die Cloud-Standardeinstellung in Ordnung. Die vollständig lokale Konfiguration lohnt die langsamere Zusammenfassung, wenn das Transkript selbst ein Risiko darstellt: Rechtsberatungen, HR-Untersuchungen, Vorstands- und Transaktionsgespräche, Interviews mit Quellen, bei denen ein Name im Transkript jemanden den Arbeitsplatz kosten kann, sowie Patientinnen und Patienten, die ihre eigenen Arzttermine aufzeichnen, um die Aussagen der Ärztin oder des Arztes später noch einmal zu prüfen. Für einen umfassenderen Blick auf On-Device-Tools jenseits von Meetings haben wir sieben lokale KI-Tools (/de/post/best-local-ai-tools-for-productivity/) verglichen.

Die richtige Wahl hängt vom Meeting ab, nicht von der Person. Für die meisten Meetings eignet sich die Cloud-Standardeinstellung. Bei den wenigen, in denen das Transkript selbst Schaden anrichten könnte, sollten Sie eine vollständig lokale Konfiguration nutzen, sie vor dem Gespräch prüfen und offen sagen, was Sie einsetzen.

Häufig gestellte Fragen

Kann man ein KI-Notiztool nutzen, ohne etwas in die Cloud zu senden?

Ja, aber nur mit den wenigen Tools, die jeden Schritt auf Ihrer Hardware ausführen können. Ein Notiztool transkribiert Ihr Audio, analysiert das Transkript und speichert das Ergebnis. Bei jedem dieser Schritte können unabhängig Daten abfließen, und die meisten Tools führen alle drei auf fremden Servern aus. Hedy transkribiert standardmäßig auf jeder unterstützten Plattform auf dem Gerät. Auf den meisten aktuellen Geräten kann auch die Analyse lokal laufen. Wenn Cloud Sync deaktiviert ist, gelangen keine Meeting-Daten auf unsere Server, es sei denn, Sie teilen eine Sitzung ausdrücklich.

Reicht es aus zu prüfen, dass Audiodaten mein Gerät nie verlassen?

Nein, und das ist der häufigste Fehler. „Audiodaten verlassen das Gerät nie“ sagt nur aus, dass die Transkription lokal stattfindet. Das ist einer von drei Schritten. Ein Tool kann auf Ihrem Gerät transkribieren und das Transkript trotzdem an ein Sprachmodell senden. Genau das tut Hedy standardmäßig. Das Transkript ist die wortgetreue Aufzeichnung. Wird es vom Gerät übertragen, entstehen daher fast dieselben Fragen wie beim Audio. Fragen Sie nach jedem Schritt, nicht nur nach dem Mikrofon.

Erstellen KI-Notiztools Stimmabdrücke von Meeting-Teilnehmenden?

Manche tun das als Nebeneffekt der Sprecherzuordnung. Viele Systeme zur Sprechertrennung extrahieren pro Stimme ein akustisches Embedding, um Personen auseinanderzuhalten. Ob ein solches Embedding nach dem Illinois Biometric Information Privacy Act als regulierter Stimmabdruck gilt, ist eine aktuelle Prozesstheorie und keine geklärte Rechtsfrage. Zudem arbeitet nicht jedes System auf diese Weise. Steuern können Sie, wo die Zuordnung stattfindet: Bei der Sprechertrennung auf dem Gerät wird nichts übertragen.

Beseitigt die Verarbeitung auf dem Gerät biometrische Datenschutzrisiken?

Sie reduziert sie, und dafür gibt es echte Rechtsprechung. In Barnett v. Apple entschied ein Berufungsgericht in Illinois, dass Apple die biometrischen Daten der Nutzerinnen und Nutzer weder besaß noch erhob, weil sie auf deren eigenen Geräten blieben, nie an Apples Server gesendet wurden und die Funktionen optional waren und gelöscht werden konnten. Das ist ein bedeutsamer Präzedenzfall für lokale Verarbeitung, beruhte aber auf genau diesen Umständen. Es handelt sich um Risikominderung,

nicht um einen geschützten Freiraum. Über die Pflichten der Person, die das Meeting einberufen hat, sagt die Entscheidung nichts aus.

Kann ein KI-Tool das Mandatsgeheimnis beeinträchtigen?

Ein Bundesgericht hat entschieden, dass KI-generierte Dokumente weder dem Mandatsgeheimnis noch dem Schutz als anwaltliches Arbeitsergebnis unterlagen. In United States v. Heppner befand Richter Jed Rakoff, dass ein Angeklagter die Dokumente erstellt hatte, indem er Informationen seiner Anwälte in einen Chatbot eingab. Ein Grund für die Entscheidung war, dass die Datenschutzrichtlinie des Anbieters darauf hinwies, Informationen könnten in Gerichtsverfahren weitergegeben werden. Der Fall betraf einen Chatbot, den der Angeklagte selbst nutzte, und kein Meeting-Notiztool. Die Frage zu Notiztools ist damit nicht geklärt. Sprechen Sie mit Ihrer eigenen Rechtsberatung.

Macht das Deaktivieren von Cloud Sync ein Notiztool privat?

Nicht für sich allein. Die Synchronisierung regelt die Speicherung, nicht die Verarbeitung. Ein Tool kann auf seinen Servern nichts dauerhaft speichern und Ihr Audio trotzdem auf dem Weg an eine Transkriptions-API sowie Ihr Transkript an ein Sprachmodell gesendet haben. Speicherung, Transkription und Analyse sind getrennte Fragen. Beantwortet ein Anbieter nur die Frage zur Speicherung, bleiben die anderen offen.

Wie prüft man, ob ein Notiztool lokal läuft?

Der Flugmodus ist ein nützlicher erster Test, aber kein Beweis. Transkribiert ein Tool offline weiter, gibt es einen lokalen Verarbeitungsweg. Bleibt es stehen, kann das bedeuten, dass es die Cloud benötigt. Vielleicht verlangt es aber auch nur eine Anmeldung oder einen Modell-Download. Und ein Tool mit funktionierendem Offline-Weg kann wieder die Cloud nutzen, sobald Sie online sind. Ergänzen Sie den Offline-Test durch die Unterauftragsverarbeiter-Liste des Anbieters und, wenn es wirklich darauf ankommt, durch eine Prüfung des Netzwerkverkehrs.

Ist die Transkription auf dem Gerät genau genug für echte Meetings?

Für alltägliche Meetings bewährt sie sich gut. Hedys Nemotron-Engine basiert auf NVIDIAs Streaming-Sprachmodell mit 600 Millionen Parametern, läuft vollständig auf dem Gerät und ordnet das Gesagte den jeweiligen Personen zu. Die Genauigkeit hängt weiterhin von Akzent, Hintergrundgeräuschen, gleichzeitigem Sprechen und Fachvokabular ab. Testen Sie sie deshalb in Ihren eigenen Meetings, statt irgendeinem Benchmark zu vertrauen, auch unserem.

Ist ein gerätebasiertes Notiztool weniger transparent als ein Meeting-Bot?

Ja, und das spricht gegen Tools wie unseres. Ein Bot macht sich in der Teilnehmendenliste sichtbar. Eine App auf dem Telefon einer Person kündigt sich überhaupt nicht an. Dadurch werden heimliche Aufnahmen leichter, nicht schwerer. The Associated Press hat genau darauf hingewiesen. Lokale Verarbeitung regelt, wohin Daten gelangen. Sie sagt nichts darüber aus, ob die Beteiligten zugestimmt haben. Das sind getrennte Pflichten, und die zweite besteht weiterhin.

Was sendet Hedy standardmäßig an die Cloud?

Die Spracherkennung läuft auf jeder Plattform auf Ihrem Gerät, sodass Audiodaten standardmäßig nicht übertragen werden. Der Analyseschritt, der Zusammenfassungen und Vorschläge erstellt, läuft standardmäßig in der Cloud. Dort werden Transkriptinhalte vorübergehend verarbeitet und nicht zum Trainieren von Modellen verwendet. Diese Voreinstellung ist ein bewusster Kompromiss zugunsten einer

breiten Geräteunterstützung und hoher Ergebnisqualität. Mit Local AI Processing (/de/help/local-ai-processing/) können Sie die Analyse auf das Gerät verlagern. Wenn Sie außerdem Cloud Sync deaktivieren, wird nichts synchronisiert.

Kostet lokale Verarbeitung extra?

Nein. Spracherkennung auf dem Gerät und Local AI Processing sind Bestandteile des Produkts und keine eigene Datenschutzstufe. Der kostenlose Tarif umfasst 300 Minuten pro Monat. Pro kostet $12.99 pro Monat oder $99.99 pro Jahr. Lokale Modelle werden einmalig heruntergeladen und nicht pro Minute abgerechnet. Für den vollständig lokalen Weg entstehen daher keine Nutzungskosten. Aktuelle Tarife finden Sie unter Preise (/de/pricing/) .

Hedy AI · Live-KI-Coaching für wichtige Gespräche

Hedy kostenlos testen: https://www.hedy.ai/de/downloads/

https://www.hedy.ai/de/post/how-to-use-ai-meeting-notes-privately/