

Rechtliche Einordnung von KI-Tools im Film- und Content-Kontext

ChatGPT · ElevenLabs · Adobe Premiere / Firefly / AI Assistant

Stand: 05.07.2026

Fokus: Deutschland / Europäische Union

Zielgruppe: depak | Quadriga Seminar | KI in der Videoproduktion: Filme effizienter umsetzen & kreativer erzählen

Kontakt: Marcel Wehn | www.marcelwehn.de

Hinweis: Dieses Dokument bietet eine verständliche Orientierung. Es ersetzt keine individuelle Rechtsberatung.

Inhaltsverzeichnis

1. Kurzüberblick
 2. Rechtlicher Grundrahmen
 - 2.1 Datenschutz und DSGVO
 - 2.2 Fotos, Videos und biometrische Daten
 - 2.3 Stimmen, Voice Cloning und Persönlichkeitsrecht
 - 2.4 Mitarbeitende im Unternehmen
 - 2.5 Recht am eigenen Bild
 - 2.6 AI Act und Kennzeichnungspflichten
 - 2.7 Urheberrecht an KI-generiertem Material
 3. Tool-Einordnung
 - 3.1 ChatGPT / OpenAI
 - 3.2 ElevenLabs
 - 3.3 Adobe Premiere / Adobe Firefly / Adobe AI Assistant
 4. Upload von Fotos, Videos und Stimmen echter Personen
 5. Rechte am KI-generierten Material
 6. Besondere Einordnung: Stimmen aus der ElevenLabs Voice Library
 7. Praktische Checkliste für Unternehmen
 8. Zusammenfassende Orientierung
 9. Quellen und weiterführende Links
-

1. Kurzüberblick

Die wichtigste Grundregel lautet:

Eine Tool-Lizenz ersetzt keine Personenrechte.

Viele KI-Plattformen erlauben ihren Nutzerinnen und Nutzern eine weitgehende Nutzung des erzeugten Outputs. Das bedeutet jedoch nicht automatisch, dass alle Rechte an Fotos, Videos, Stimmen, Marken, Musik, Unternehmensmaterial oder erkennbaren Personen geklärt sind.

Für Unternehmen ist deshalb folgende Unterscheidung entscheidend:

Komplett neu erzeugtes KI-Material ist häufig einfacher nutzbar als KI-Material, das auf echten Menschen, echten Stimmen, echten Fotos oder echtem Videomaterial basiert.

Besonders sensibel sind:

- Fotos und Videos von Mitarbeitenden,
- Stimmufnahmen echter Personen,
- Voice Cloning,
- KI-Dubbing,
- Avatare,
- Bild-zu-Video-Anwendungen mit echten Personen,
- werbliche oder kommerzielle Nutzung,
- Uploads über private Accounts,
- Verarbeitung vertraulicher Kunden- oder Unternehmensdaten.

Die praktische Kurzform lautet:

Was rechtlich nicht aufgenommen, gespeichert, verändert oder veröffentlicht werden darf, sollte auch nicht ohne weitere Prüfung in ein KI-Tool hochgeladen werden.

2. Rechtlicher Grundrahmen

2.1 Datenschutz und DSGVO

Fotos, Videos, Stimmen, Transkripte, Namen, Projektinformationen und Metadaten können personenbezogene Daten sein, wenn eine Person direkt oder indirekt identifiziert werden kann. Die DSGVO definiert personenbezogene Daten weit und erfasst alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Der Upload in ein KI-Tool ist regelmäßig eine Verarbeitung personenbezogener Daten. Die DSGVO versteht unter Verarbeitung unter anderem das Erheben, Speichern, Anpassen, Verändern, Verwenden, Offenlegen oder Übermitteln personenbezogener Daten.

Für eine solche Verarbeitung braucht das Unternehmen eine Rechtsgrundlage. In Betracht kommen insbesondere Einwilligung, Vertragserfüllung, rechtliche Pflicht oder berechtigtes

Interesse. Zusätzlich gelten die Grundsätze der Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung und Sicherheit der Verarbeitung.

Wenn ein KI-Anbieter personenbezogene Daten im Auftrag eines Unternehmens verarbeitet, ist in der Regel ein Auftragsverarbeitungsvertrag beziehungsweise Data Processing Addendum erforderlich. Die DSGVO regelt diese Anforderungen in Art. 28.

Die Datenschutzkonferenz empfiehlt, vor dem Einsatz einer KI-Anwendung die konkreten Einsatzfelder und Zwecke festzulegen, die datenschutzrechtliche Rolle der Beteiligten zu klären und die Ergebnisse einer KI-Anwendung auf Richtigkeit zu prüfen.

2.2 Fotos, Videos und biometrische Daten

Ein normales Foto oder Video ist nicht automatisch eine besondere Kategorie personenbezogener Daten. Kritisch wird es aber, wenn Fotos, Videos oder Gesichter mit speziellen technischen Verfahren verarbeitet werden, um Personen eindeutig zu identifizieren oder zu authentifizieren. Dann kann biometrische Datenverarbeitung im Sinne von Art. 9 DSGVO betroffen sein.

Für Film- und KI-Projekte bedeutet das:

Normale Schnittbearbeitung ist anders zu bewerten als Gesichtserkennung, Avatarbildung, Gesichtsmodellierung, technische Identifikation oder das systematische Erzeugen einer digitalen Person.

2.3 Stimmen, Voice Cloning und Persönlichkeitsrecht

Auch Stimmen können personenbezogene Daten sein, wenn eine Person über die Stimme identifizierbar ist. Bei Voice Cloning oder der KI-Nachahmung einer erkennbaren Stimme kommen zusätzlich Persönlichkeitsrechte ins Spiel.

Besonders sensibel sind:

- das Klonen einer Mitarbeitendenstimme,
- das Verändern einer echten Stimme,
- KI-Dubbing mit erkennbarer Originalstimme,
- synthetische Übersetzungen mit gleicher Stimmidentität,
- der Einsatz einer geklonten Stimme in Werbung, PR, Recruiting oder Vertrieb.

Die praktische Konsequenz lautet:

Wenn eine Stimme einer echten Person zugeordnet werden kann oder bewusst wie diese Person klingen soll, sollte vor der Nutzung eine ausdrückliche Zustimmung eingeholt werden.

2.4 Mitarbeitende im Unternehmen

Bei Mitarbeitenden ist besondere Vorsicht geboten. Im Arbeitsverhältnis ist eine Einwilligung nicht automatisch freiwillig, weil ein Machtgefälle zwischen Arbeitgeber und Beschäftigten bestehen kann. Der Europäische Datenschutzausschuss betont, dass eine wirksame Einwilligung freiwillig, spezifisch, informiert und eindeutig sein muss.

Nach § 26 BDSG kann eine Einwilligung im Beschäftigungskontext grundsätzlich möglich sein. Sie muss jedoch freiwillig erfolgen und in der Regel schriftlich oder elektronisch dokumentiert werden.

Für KI-Filmprojekte bedeutet das:

Eine allgemeine Zustimmung zur Aufnahme eines Interviews reicht nicht automatisch für Voice Cloning, KI-Dubbing, Avatarbildung, werbliche Nutzung, Paid Ads oder internationale Veröffentlichung.

2.5 Recht am eigenen Bild

Nach § 22 Kunsturhebergesetz dürfen Bildnisse grundsätzlich nur mit Einwilligung der abgebildeten Person verbreitet oder öffentlich zur Schau gestellt werden.

Das betrifft insbesondere:

- Unternehmensvideos,
- Recruitingfilme,
- Social-Media-Clips,
- Eventfilme,
- Kundenreferenzen,
- Werbematerial,
- KI-generierte Varianten echter Personen.

Auch wenn es Ausnahmen gibt, etwa für Personen als Beiwerk oder Bilder von Versammlungen, sollten diese Ausnahmen bei KI-Bearbeitung, werblicher Nutzung und gezielter Darstellung von Mitarbeitenden nicht pauschal angenommen werden.

2.6 AI Act und Kennzeichnungspflichten

Der EU AI Act enthält Transparenzpflichten für bestimmte KI-Systeme und KI-Inhalte. Besonders relevant ist Art. 50 AI Act. Danach müssen Betreiber eines KI-Systems offenlegen, wenn Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert werden und einen Deepfake darstellen.

Die Europäische Kommission weist darauf hin, dass die Transparenzregeln nach Art. 50 ab dem 2. August 2026 anwendbar werden. Dazu gehören unter anderem Hinweise bei Deepfakes und Transparenzpflichten für KI-generierte oder manipulierte Inhalte.

Für Film, Marketing, PR und Social Media bedeutet das:

Wenn ein Inhalt echt wirken kann, tatsächlich aber künstlich erzeugt oder wesentlich durch KI manipuliert wurde, sollte geprüft werden, ob eine Kennzeichnung erforderlich ist.

2.7 Urheberrecht an KI-generiertem Material

Bei rein KI-generierten Inhalten ist nicht automatisch klar, ob daran ein vollwertiges Urheberrecht entsteht. Auf EU-Ebene gibt es bislang keine spezifischen Regeln zur urheberrechtlichen Schutzfähigkeit vollständig KI-generierter Werke. Nach der aktuellen europäischen Diskussion bleibt menschliche Kreativität ein zentrales Kriterium.

Praktisch bedeutet das:

Ein Unternehmen kann KI-Output aufgrund der Tool-Lizenz häufig nutzen. Es sollte aber nicht automatisch davon ausgehen, dass dieser Output exklusiv geschützt ist oder dass andere keine ähnlichen Inhalte erzeugen können.

3. Tool-Einordnung

3.1 ChatGPT / OpenAI

Datenschutz und DSGVO

Bei privaten ChatGPT-Zugängen wie Free, Plus oder Pro ist besondere Vorsicht geboten, wenn Unternehmensdaten, Kundendaten oder personenbezogene Daten verarbeitet werden. OpenAI erklärt, dass Inhalte aus Verbraucherangeboten zur Verbesserung der Modelle verwendet werden können, sofern Nutzerinnen und Nutzer dies nicht über die entsprechenden Einstellungen deaktivieren.

Bei ChatGPT Business, ChatGPT Enterprise und API gilt eine andere Ausgangslage. OpenAI erklärt, dass Daten aus Business-Angeboten und der API standardmäßig nicht zum Training oder zur Verbesserung der Modelle verwendet werden.

OpenAI stellt für Geschäftskunden ein Data Processing Addendum bereit. Dieses ist für datenschutzrechtliche Unternehmensprozesse relevant, wenn personenbezogene Daten im Rahmen einer Auftragsverarbeitung verarbeitet werden.

Unterschied zwischen privatem Account und Business-Zugang

Der Unterschied zwischen privatem Zugang und Business-Zugang liegt nicht nur im Preis oder Funktionsumfang, sondern vor allem in Datenschutz, Governance und Steuerbarkeit.

Privater Account / Plus / Pro

- primär für individuelle Nutzung gedacht,
- Datenverwendung zur Modellverbesserung je nach Einstellung möglich,
- keine zentrale Unternehmenssteuerung,
- keine vergleichbare Admin-, Rollen- und Rechteverwaltung,
- für vertrauliches Unternehmensmaterial, Kundendaten oder Mitarbeitendendaten nur eingeschränkt geeignet.

ChatGPT Business / Enterprise / API

- auf Unternehmensnutzung ausgelegt,
- Business-Daten werden nach OpenAI-Angaben standardmäßig nicht zum Training genutzt,
- DPA / AVV verfügbar,

- zentrale Verwaltung und Sicherheitsfunktionen möglich,
- bessere Grundlage für interne Richtlinien, Freigabeprozesse und Compliance.

Für Unternehmen lautet die praktische Empfehlung:

Personenbezogene, vertrauliche oder unternehmensrelevante Inhalte sollten nicht über private Accounts verarbeitet werden. Für Unternehmenszwecke sollte ein Business-, Enterprise- oder API-Setup mit interner Nutzungsrichtlinie eingesetzt werden.

Upload von Fotos, Videos und Stimmen

Bei Uploads von Bildern, Videos oder Stimmen mit echten Personen bleibt das Unternehmen dafür verantwortlich, dass die notwendigen Rechte, Einwilligungen und Rechtsgrundlagen vorliegen.

OpenAI weist in den Service Terms darauf hin, dass visuelle Funktionen nicht genutzt werden dürfen, um die Ähnlichkeit einer Person ohne ausdrückliche Zustimmung und notwendige Rechte zu reproduzieren.

Besonders wichtig ist außerdem der Umgang mit ChatGPT Voice Output. OpenAI regelt in den Service Terms, dass ChatGPT Voice Output nur für nicht-kommerzielle Nutzung bestimmt ist und nicht als eigenständige Audiodatei verbreitet oder neu verpackt werden darf. Die allgemeine Rechteübertragung am Output umfasst diesen Voice Output ausdrücklich nicht.

Rechte am Output

OpenAI regelt in den Nutzungsbedingungen, dass Nutzerinnen und Nutzer im Verhältnis zu OpenAI Rechte am Input behalten und Rechte am Output erhalten, soweit dies rechtlich zulässig ist.

Für Geschäftskunden stellt OpenAI außerdem klar, dass Kundinnen und Kunden für die Nutzung von Outputs und für die Bewertung von Richtigkeit und Angemessenheit des Outputs verantwortlich bleiben.

Das bedeutet:

OpenAI überträgt im Verhältnis zur Plattform weitgehend Rechte am Output. Das ersetzt aber nicht die Prüfung, ob der Output Rechte Dritter verletzt, personenbezogene Daten enthält, eine echte Person nachbildet, vertrauliche Informationen offenlegt oder für Werbung rechtlich freigegeben ist.

Einordnung für Unternehmen

ChatGPT ist für Unternehmen rechtlich am sichersten, wenn es über Business, Enterprise oder API mit AVV/DPA, interner Nutzungsrichtlinie und klaren Datenschutzvorgaben eingesetzt wird.

Für Seminarkontexte lässt sich die Einordnung so zusammenfassen:

Geeignet: Ideenentwicklung, Skriptentwürfe, Zusammenfassungen, Textvarianten, Konzeptarbeit ohne personenbezogene oder vertrauliche Daten.

Nur mit Prüfung geeignet: Verarbeitung von Fotos, Stimmen, Videos, Transkripten, Kundendaten oder Mitarbeitendeninformationen.

Nicht empfehlenswert: Upload vertraulicher Unternehmensdaten oder personenbezogener Mitarbeitendendaten in private Accounts.

3.2 ElevenLabs

Datenschutz und DSGVO

ElevenLabs ist besonders sensibel, weil das Tool stark mit Stimmen, Audio, Voice Cloning, Dubbing sowie Bild- und Videoanwendungen verbunden ist.

Der ElevenLabs Data Processing Addendum beschreibt, dass ElevenLabs personenbezogene Kundendaten als Auftragsverarbeiter verarbeiten kann. Als mögliche Kategorien personenbezogener Daten werden unter anderem Audio- oder Videoaufnahmen, Texteingaben und sonstige hochgeladene Inhalte genannt.

Der DPA stellt außerdem klar, dass Kundinnen und Kunden für notwendige Hinweise und Einwilligungen gegenüber betroffenen Personen verantwortlich sind.

ElevenLabs weist in seiner Datenschutzerklärung darauf hin, dass bei Professional Voice Cloning Audioaufnahmen und Voice Data verarbeitet werden können, um zu verifizieren, dass es sich um die eigene Stimme handelt beziehungsweise dass eine Zustimmung zur Nutzung durch Dritte vorliegt.

Upload von Stimmen, Fotos und Videos

Bei Stimmen echter Personen ist eine ausdrückliche Zustimmung besonders wichtig. ElevenLabs weist im Kontext Text-to-Speech und Voice Cloning darauf hin, dass für das Klonen einer Stimme eine Erlaubnis erforderlich ist.

Für Unternehmen bedeutet das:

Eine Mitarbeitendenstimme sollte nur dann geklont, verändert, übersetzt oder in einer anderen Sprache synthetisch nachgebildet werden, wenn die betroffene Person vorher konkret zugestimmt hat.

Die Zustimmung sollte mindestens regeln:

- welche Stimme genutzt wird,
- welches Ausgangsmaterial verwendet wird,
- mit welchem Tool gearbeitet wird,
- ob die Stimme geklont, verändert, übersetzt oder synchronisiert wird,
- für welche Inhalte und Kanäle die Stimme eingesetzt wird,
- ob interne, öffentliche, werbliche oder kommerzielle Nutzung erlaubt ist,
- wie lange die Nutzung erlaubt ist,
- ob Paid Ads, Recruiting, Vertrieb oder PR umfasst sind,
- wie Widerruf, Löschung und Ausscheiden aus dem Unternehmen behandelt werden.

Kommerzielle Nutzung

ElevenLabs unterscheidet deutlich zwischen kostenloser und bezahlter Nutzung. Nach der ElevenLabs-Hilfe enthält der Free Plan keine kommerzielle Lizenz. Bezahlte Pläne enthalten grundsätzlich eine kommerzielle Lizenz, sofern keine Beta Services genutzt werden und alle sonstigen Bedingungen eingehalten werden. Inhalte aus Beta Services dürfen nach ElevenLabs-Angaben nicht kommerziell oder in Produktionsumgebungen genutzt werden.

Das bedeutet:

Eine kommerzielle Tool-Lizenz erlaubt nicht automatisch die Nutzung einer echten Person oder echten Stimme. Sie regelt zunächst nur das Verhältnis zur Plattform. Persönlichkeitsrechte, Datenschutz und Rechte am Input bleiben separat zu prüfen.

Bild- und Video-Anwendungen

ElevenLabs hat eigene Image & Video Terms veröffentlicht. Diese gelten ergänzend für die Nutzung entsprechender Bild- und Videofunktionen und verweisen ebenfalls auf Nutzungsbedingungen, Datenschutzregeln und Prohibited Use Policy.

Für Bild-zu-Video, Videoveränderungen oder KI-Bearbeitung echter Personen gilt deshalb:

Es müssen sowohl Datenschutz als auch Persönlichkeitsrechte und Rechte am Ausgangsmaterial geprüft werden. Besonders heikel sind täuschende Darstellungen, Deepfake-ähnliche Inhalte, synthetische Aussagen echter Personen oder werbliche Nutzungen ohne klare Einwilligung.

Einordnung für Unternehmen

ElevenLabs ist für Unternehmen nutzbar, aber rechtlich besonders sensibel. Das liegt vor allem daran, dass Stimme eng mit Identität, Wiedererkennbarkeit und Vertrauen verbunden ist.

Für Seminarkontexte lässt sich die Einordnung so zusammenfassen:

Geeignet: generische KI-Stimmen, lizenzierte Voice-Library-Stimmen, interne Entwürfe, nicht-personenbezogene Voiceovers im bezahlten Plan.

Nur mit Prüfung geeignet: Mitarbeitendenstimmen, Dubbing, Voice Changer, Bild-zu-Video mit echten Personen, Avatar- oder Deepfake-nahe Anwendungen.

Nicht empfehlenswert: Voice Cloning ohne ausdrückliche Zustimmung, Imitation von Kolleginnen, Kollegen, Prominenten oder Kundinnen und Kunden, täuschende synthetische Aussagen.

3.3 Adobe Premiere / Adobe Firefly / Adobe AI Assistant

Datenschutz und DSGVO

Adobe ist im Unternehmenskontext häufig besser steuerbar als reine Consumer-Tools, weil Creative Cloud for Teams oder Enterprise, Admin-Funktionen und Vertragsunterlagen verfügbar sind. Entscheidend ist jedoch immer die konkrete Funktion.

Adobe erklärt in den Nutzungsbedingungen, dass lokal gespeicherte Inhalte nicht gescannt oder geprüft werden. Außerdem erklärt Adobe, generative KI-Modelle nicht mit Inhalten von Nutzerinnen und Nutzern oder deren Kundinnen und Kunden zu trainieren, sofern diese Inhalte nicht beispielsweise in Adobe Stock eingebracht werden.

Adobe erklärt in der Content Analysis FAQ, dass Nutzerinnen und Nutzer mit Business-Profil beziehungsweise Business-Account automatisch von Content Analysis zur Produktverbesserung abgemeldet sind.

Das bedeutet jedoch nicht, dass jeder Adobe-Workflow automatisch datenschutzfrei ist. Cloud-Speicherung, Transkription, Frame.io, Firefly-Funktionen, Media Intelligence oder AI Assistant können je nach Funktion Cloud-Verarbeitung auslösen.

Premiere, KI-Funktionen und Version 26.x / 26.5

Adobe dokumentiert für Premiere neue KI-Funktionen wie Generative Extend, Media Intelligence und Translate Captions. Generative Extend kann Frames am Anfang oder Ende eines Clips hinzufügen. Media Intelligence ermöglicht die Suche über visuelle Inhalte, Transkripte und Metadaten.

Der Premiere AI Assistant ist von Adobe als Beta-Funktion beschrieben. Er soll repetitive Schnittaufgaben reduzieren, Medien organisieren, Footage vorbereiten und erste Schnittfassungen direkt in Premiere unterstützen.

Adobe beschreibt außerdem, dass der AI Assistant in Premiere als Beta-Funktion in einfachen Prompts Workflows beschleunigen, Footage organisieren und Timelines verwalten kann.

Zur von Ihnen genannten Version 26.5 ist wichtig:

Nach den auffindbaren Adobe-Quellen und Community-Hinweisen taucht Premiere Beta 26.5 im Beta-Kontext auf, etwa bei Audio-Ducking-Updates. Für die rechtliche Bewertung ist deshalb weniger die Versionsnummer entscheidend, sondern ob die konkrete Funktion lokal arbeitet, Cloud-Verarbeitung auslöst, Beta ist oder generative KI nutzt.

Kommerzielle Nutzung von Firefly-Output

Adobe erklärt in der Firefly FAQ, dass Ausgaben aus Firefly-Funktionen ohne Beta-Label für kommerzielle Projekte genutzt werden können. Bei Beta-Funktionen ist kommerzielle Nutzung ebenfalls möglich, sofern im Produkt nicht ausdrücklich etwas anderes angegeben ist.

Adobe weist zudem darauf hin, dass Firefly-generierte Outputs in vielen Kontexten als kommerziell nutzbar betrachtet werden, bei Partner-Modellen jedoch zusätzliche Prüfung erforderlich sein kann.

Das bedeutet:

Adobe Firefly kann für kommerzielle Projekte eine gute Grundlage sein. Dennoch ersetzt Adobe keine Rechte an Personen, Marken, Musik, Logos, Stockmaterial, Kundenmaterial oder vertraulichem Input.

Einordnung für Unternehmen

Adobe Premiere ist für Unternehmen grundsätzlich gut in professionelle Workflows integrierbar. Rechtlich bleibt aber entscheidend, ob Rohmaterial personenbezogene Daten enthält und ob KI-Funktionen Cloud-Verarbeitung oder generative Veränderungen auslösen.

Für Seminarkontexte lässt sich die Einordnung so zusammenfassen:

Geeignet: professioneller Schnitt in Business-/Enterprise-Umgebungen, lokale Bearbeitung, freigegebenes Rohmaterial, Firefly-Output mit kommerzieller Freigabe.

Nur mit Prüfung geeignet: KI-Transkription, Media Intelligence, Generative Extend, AI Assistant, Frame.io, Cloud-Verarbeitung mit Personenmaterial.

Nicht empfehlenswert: Nutzung von NDA-, Kunden- oder Mitarbeitendenmaterial in Beta- oder Cloud-KI-Funktionen ohne vorherige Freigabe.

4. Upload von Fotos, Videos und Stimmen echter Personen

Wenn echtes Personenmaterial in KI-Tools hochgeladen wird, sollten Unternehmen vier Ebenen prüfen.

4.1 Datenschutzrecht

Es braucht eine Rechtsgrundlage nach Art. 6 DSGVO. Bei besonders sensibler Verarbeitung, etwa biometrischer Identifikation, kann Art. 9 DSGVO relevant werden.

Bei Mitarbeitenden sollte die Rechtsgrundlage besonders sorgfältig geprüft werden. Eine Einwilligung muss freiwillig sein und darf nicht bloß formal eingeholt werden.

4.2 Persönlichkeitsrechte

Bei Fotos und Videos ist das Recht am eigenen Bild zu beachten. Bei Stimmen ist das allgemeine Persönlichkeitsrecht betroffen, insbesondere wenn eine Stimme wiedererkennbar imitiert, verändert oder geklont wird.

4.3 Rechte am Ausgangsmaterial

Das Unternehmen muss klären, ob es das Ausgangsmaterial überhaupt verwenden darf. Das betrifft:

- Fotos,
- Videos,
- Tonaufnahmen,
- Musik,
- Logos,
- Marken,
- Stockmaterial,
- Kundendaten,
- Agenturmaterial,
- Archivmaterial,
- NDA-geschützte Inhalte.

Eine KI-Plattform kann nur Nutzungsrechte am Verhältnis zwischen Plattform und Nutzerin beziehungsweise Nutzer regeln. Sie kann fehlende Rechte am Ausgangsmaterial nicht ersetzen.

4.4 Zweckbindung

Eine Zustimmung für einen normalen Videodreh bedeutet nicht automatisch Zustimmung zu KI-Bearbeitung, Voice Cloning, KI-Dubbing, Avatarbildung, internationaler Veröffentlichung oder Paid Ads.

Deshalb sollte der Zweck konkret beschrieben werden. Eine gute Zustimmung unterscheidet beispielsweise zwischen:

- interner Nutzung,
 - Schulung,
 - Website,
 - Social Media,
 - PR,
 - Recruiting,
 - Vertrieb,
 - Paid Advertising,
 - internationaler Veröffentlichung,
 - KI-Veränderung,
 - KI-generierter Nachbildung.
-

5. Rechte am KI-generierten Material

5.1 Komplett neu erzeugte Fotos, Videos oder Stimmen

Bei vollständig neu erzeugten Inhalten ist die Nutzung häufig einfacher, wenn der gebuchte Tool-Plan kommerzielle Nutzung erlaubt.

Das gilt insbesondere für:

- neu generierte Bilder ohne reale Vorlage,
- generische KI-Stimmen,
- abstrakte oder illustrative Videos,
- Text-, Konzept- und Skriptoutputs,
- generische Voiceovers ohne Nachbildung einer konkreten Person.

Trotzdem bleiben Risiken:

- Der Output kann einer echten Person ähneln.
- Der Output kann Marken, Logos oder Designs enthalten.
- Der Output kann urheberrechtlich geschützte Elemente imitieren.
- Der Output kann nicht exklusiv sein.
- Der Output kann nicht oder nur eingeschränkt urheberrechtlich geschützt sein.
- Eine KI-Kennzeichnung kann erforderlich sein.

5.2 Fotos, Videos oder Stimmen echter Menschen als Grundlage

Wenn KI-Material auf echten Menschen basiert, ist die Lage deutlich sensibler.

Dann braucht das Unternehmen in der Regel zusätzlich:

- Einwilligung zur Aufnahme,
- Einwilligung zur Veröffentlichung,
- Einwilligung zur KI-Bearbeitung,
- Einwilligung zur kommerziellen Nutzung,
- separate Zustimmung für Voice Cloning,
- separate Zustimmung für Dubbing oder Stimmveränderung,
- separate Zustimmung für Avatarbildung oder synthetische Nachbildung,
- Regelung zu Kanälen, Dauer, Ländern und Widerruf,
- gegebenenfalls finale Freigabe durch die betroffene Person.

Die einfache Faustregel lautet:

Wenn eine echte Person erkennbar ist oder erkennbar nachgebildet wird, sollte das Ergebnis rechtlich wie eine Nutzung dieser Person behandelt werden.

5.3 Nutzung, Verbreitung, Marketing und PR

Für Öffentlichkeitsarbeit, Marketing, PR und Werbung genügt es nicht, dass ein Tool „commercial use“ erlaubt.

Zusätzlich sollten folgende Fragen geklärt werden:

- Darf das Unternehmen das Inputmaterial verwenden?
 - Sind abgebildete oder hörbare Personen einverstanden?
 - Ist KI-Bearbeitung ausdrücklich umfasst?
 - Dürfen Inhalte weltweit online veröffentlicht werden?
 - Sind Paid Ads, Recruiting, Vertrieb oder Messekommunikation erlaubt?
 - Enthält der Output Marken, Musik, Stockmaterial oder geschützte Designs?
 - Ist eine Kennzeichnung als KI-generiert oder KI-manipuliert erforderlich?
 - Ist eine menschliche Prüfung erfolgt?
-

6. Besondere Einordnung: Stimmen aus der ElevenLabs Voice Library

ElevenLabs bietet Stimmen über eine Voice Library an. Die Voice Library ist ein Marktplatz, auf dem die Community Professional Voice Clones teilen kann. Andere Nutzerinnen und Nutzer können diese Stimmen verwenden, während die Erstellerinnen und Ersteller dafür Vergütungen erhalten können.

Das Voice Library Addendum beschreibt, dass die Nutzung der Voice Library zusätzlichen Bedingungen unterliegt. Wer ein Voice Model in die Voice Library stellt, muss über die notwendigen Rechte verfügen und darf keine fremde Stimme ohne entsprechende Rechte bereitstellen.

Für Unternehmen ist wichtig:

Die Voice Library ist keine exklusive Sprecherbuchung. Sie ist eine Plattformlizenz. Für viele Social-Media-Clips, Erklärvideos, interne Anwendungen oder kleinere Produktionen kann das ausreichend sein, wenn der passende Plan kommerzielle Nutzung erlaubt.

Für größere oder längerfristige Nutzungen sollte jedoch genauer geprüft werden, insbesondere bei:

- TV-Kampagnen,
- großen Paid-Ads-Kampagnen,
- langfristiger Markenstimme,
- sensiblen Branchen,
- politischer Kommunikation,
- Healthcare,
- Finanzkommunikation,
- Arbeitgebermarke,
- internationalen Kampagnen.

Bei ElevenLabs gilt außerdem: Der Free Plan enthält nach Anbieterangaben keine kommerzielle Lizenz. Bezahlte Pläne enthalten grundsätzlich eine kommerzielle Lizenz, sofern keine Beta Services genutzt werden und die sonstigen Bedingungen eingehalten werden.

Praktische Empfehlung:

Für kurzfristige, einfache Inhalte kann die Voice Library ausreichend sein. Für eine dauerhafte Markenstimme oder größere Kampagnen sollte eine gesonderte Rechteklärung beziehungsweise eine direkte Sprecherlizenz geprüft werden.

7. Praktische Checkliste für Unternehmen

Vor dem Einsatz von KI-Tools mit Film-, Foto-, Video- oder Audiomaterial sollten Unternehmen folgende Punkte prüfen:

1. Wird ein Business-, Team- oder Enterprise-Zugang genutzt?
2. Gibt es einen AVV beziehungsweise DPA mit dem Anbieter?
3. Ist klar, ob Daten zum Training genutzt werden können?
4. Werden personenbezogene Daten minimiert?
5. Sind Mitarbeitende oder andere Personen informiert?
6. Liegt eine ausreichende Einwilligung oder andere Rechtsgrundlage vor?
7. Ist die KI-Bearbeitung ausdrücklich umfasst?
8. Sind Stimme, Voice Clone, Dubbing oder Avatar separat geregelt?
9. Ist kommerzielle Nutzung durch den Tool-Plan erlaubt?
10. Sind Marken, Musik, Stockmaterial, Logos und Kundenrechte geklärt?
11. Ist eine KI-Kennzeichnung erforderlich?
12. Gibt es eine menschliche Endprüfung vor Veröffentlichung?

Mindestinhalte einer Zustimmung bei Mitarbeitendenmaterial

Eine Zustimmung sollte klar regeln:

- welche Fotos, Videos oder Stimmen genutzt werden,
- mit welchen KI-Tools gearbeitet wird,
- ob Material verändert, verlängert, übersetzt, geklont oder als Avatar genutzt wird,

- für welche Zwecke die Nutzung erfolgt,
- ob Marketing, PR, Werbung oder Paid Ads erlaubt sind,
- für welche Kanäle und Länder die Nutzung gilt,
- wie lange die Nutzung erlaubt ist,
- ob eine finale Freigabe erforderlich ist,
- wie Widerruf und Löschung geregelt sind,
- was beim Ausscheiden aus dem Unternehmen gilt.

Besonders wichtig:

Voice Cloning, Avatar-Nutzung und täuschend echte KI-Darstellungen sollten immer separat und ausdrücklich geregelt werden.

8. Zusammenfassende Orientierung

ChatGPT

ChatGPT ist für Unternehmen am besten über Business, Enterprise oder API geeignet. Private Accounts sollten nicht für vertrauliche Unternehmensdaten, Kundendaten oder personenbezogenes Mitarbeitendenmaterial genutzt werden.

Kernrisiko: Upload sensibler Daten in ungeeignete Accounts.

Kernmaßnahme: Business-Setup, DPA/AVV, interne Nutzungsrichtlinie, keine unnötigen personenbezogenen Daten.

Besonderheit: ChatGPT Voice Output ist nach OpenAI Service Terms nur nicht-kommerziell nutzbar und nicht als eigenständige Audiodatei zur Verbreitung gedacht.

ElevenLabs

ElevenLabs ist besonders sensibel, weil Stimme ein stark identitätsbezogenes Merkmal ist. Bei generischen Stimmen oder korrekt lizenzierte Voice-Library-Nutzung ist die Nutzung eher beherrschbar. Bei Voice Cloning, Dubbing und Mitarbeitendenstimmen ist besondere Vorsicht geboten.

Kernrisiko: Nutzung oder Nachbildung echter Stimmen ohne ausdrückliche Zustimmung.

Kernmaßnahme: schriftliches Voice Release, bezahlter Plan für kommerzielle Nutzung, keine Beta Services für Produktion.

Besonderheit: Free Plan ohne kommerzielle Lizenz; bezahlte Pläne grundsätzlich mit kommerzieller Lizenz, sofern Bedingungen eingehalten werden.

Adobe Premiere / Firefly / AI Assistant

Adobe Premiere ist im professionellen Unternehmensworkflow gut integrierbar. Dennoch bleiben Rohmaterial, Stimmen, Gesichter und Kundendaten personenbezogen und rechtopflichtig. KI-Funktionen können je nach Funktion Cloud-Verarbeitung oder generative Bearbeitung auslösen.

Kernrisiko: Personen- oder Kundenmaterial in Cloud-, Beta- oder generative KI-Funktionen ohne Freigabe.

Kernmaßnahme: Business-/Enterprise-Setup, Prüfung konkreter Funktion, Freigabe des Rohmaterials, klare interne Workflows.

Besonderheit: Adobe erklärt, generative KI-Modelle nicht mit Kundinnen- und Kundeninhalten zu trainieren, sofern diese nicht beispielsweise in Adobe Stock eingebracht werden.

9. Quellen und weiterführende Links

Rechtsgrundlagen

DSGVO / Datenschutz-Grundverordnung

Relevant für personenbezogene Daten, Rechtsgrundlagen der Verarbeitung, besondere Kategorien personenbezogener Daten, Informationspflichten und Auftragsverarbeitung.

§ 26 BDSG – Beschäftigtendatenschutz

Relevant für Verarbeitung personenbezogener Daten von Beschäftigten und Einwilligungen im Arbeitsverhältnis.

§ 22 Kunsturhebergesetz – Recht am eigenen Bild

Relevant für Veröffentlichung und öffentliche Zurschaustellung von Bildnissen.

EU AI Act, Art. 50 – Transparenzpflichten

Relevant für Deepfakes, KI-generierte oder KI-manipulierte Bild-, Ton- und Videoinhalte.

Europäische Kommission – Transparenzregeln des AI Act

Relevant für Anwendbarkeit der Transparenzpflichten ab 2. August 2026.

Datenschutzkonferenz – Orientierungshilfe KI und Datenschutz

Relevant für Zweckbestimmung, Auswahl von KI-Anwendungen, Verantwortlichkeit und Prüfung von Ergebnissen.

Europäischer Datenschutzausschuss – Guidelines on Consent

Relevant für Anforderungen an wirksame Einwilligung.

Europäisches Parlament – Copyright of AI-generated works

Relevant für die Einordnung, dass die EU bislang keine spezifischen Regeln zur Schutzfähigkeit KI-generierter Werke hat und menschliche Kreativität weiterhin zentral ist.

Anbieterquellen: OpenAI / ChatGPT

OpenAI Business Data Privacy

Relevant für die Aussage, dass Business- und API-Daten standardmäßig nicht zum Training genutzt werden.

OpenAI ChatGPT Business Privacy

Relevant für Business-Daten, Verschlüsselung und Ausschluss vom Training.

OpenAI Data Processing Addendum

Relevant für Auftragsverarbeitung und Datenschutzverträge.

OpenAI Terms of Use / EU Terms of Use
Relevant für Rechte an Input und Output.

OpenAI Service Terms
Relevant für Visual Capabilities und ChatGPT Voice Output.

Anbieterquellen: ElevenLabs

ElevenLabs Data Processing Addendum
Relevant für Auftragsverarbeitung, Customer Personal Data, Audio-/Videoaufnahmen und Kundenzuständigkeit für Hinweise und Einwilligungen.

ElevenLabs Privacy Policy
Relevant für Voice Data und Verifizierung bei Professional Voice Cloning.

ElevenLabs Commercial Use Help Article
Relevant für Free Plan, bezahlte Pläne, kommerzielle Nutzung und Beta Services.

ElevenLabs Voice Library Documentation
Relevant für die Einordnung der Voice Library als Marktplatz für Professional Voice Clones.

ElevenLabs Voice Library Addendum
Relevant für zusätzliche Bedingungen der Voice Library.

ElevenLabs Image & Video Terms
Relevant für Bild- und Videofunktionen.

Anbieterquellen: Adobe

Adobe General Terms of Use
Relevant für Aussagen zu lokal gespeicherten Inhalten und Training generativer KI-Modelle.

Adobe Content Analysis FAQ
Relevant für Content Analysis und automatisches Opt-out bei Business-Profilen.

Adobe Premiere Release Notes / What's New
Relevant für Generative Extend, Media Intelligence und weitere KI-Funktionen in Premiere.

Adobe Premiere AI Assistant Overview
Relevant für die Einordnung des AI Assistant als Beta-Funktion.

Adobe Firefly FAQ
Relevant für kommerzielle Nutzung von Firefly-Outputs.

Adobe Premiere AI Assistant FAQ
Relevant für Firefly-Outputs, Partner-Modelle und kommerzielle Nutzung.