WAWAYARO

WHITEPAPER

KI IM KUNDENEINSATZ

Was ich prüfen musste, bevor ich es guten Gewissens tun konnte

Ein Erfahrungsbericht aus einer kleinen GmbH – mit Werkzeug-Anhang für den europäischen Rechtsraum

Andreas Riedel · Wawayaro GmbH, Berlin

FASSUNG 4 · STAND 28.11.2026 · WERKZEUG-ANHANG V2

INHALT

TEIL A – DER VORGANG 6

1. Wie es anfing 7
2. Der Befund 9
3. Warum ein Schalter im Konto kein Vertrag ist 11
4. Die Liste wurde länger, nicht kürzer 12
5. Die Tarifentscheidung – und was sich dabei nicht messen ließ 14
6. Was die Preisliste nicht zeigt 16

TEIL B – WAS ICH DARAUS GELERNT HABE 18

1. Die Trennlinie, an der sich alles entscheidet 19
2. Drei Achsen – und eine, die keine ist 21
3. Die fünf Nebenwege – der eigentliche Regelungsbedarf 22
4. Was am Auftragsverarbeitungsvertrag tatsächlich zu prüfen ist 24
5. EU-Hosting, EU-Vertragspartner, EU-Verarbeitung – drei Dinge, nicht eines 26
6. Was heute gilt – der Rechtsrahmen in einer Seite 28
7. Was eine Datenschutzerklärung nicht heilt 30
8. Kenntnis macht es besser, nicht schlechter 31
9. Die Methode – sechs Regeln, die ich seither anwende 32
10. So bin ich vorgegangen – zehn Fragen, die ich mir je Werkzeug gestellt habe 33

TEIL C – WERKZEUG-ANHANG, STAND 27.11.2026 (V2) 36

C.1 KI-Assistenten im Chat 38
C.2 Programmierschnittstellen und Coding-Werkzeuge 42
C.3 Bild- und Mediengeneratoren 45
C.4 Gesprächsaufzeichnung, Transkription, Meeting-Assistenten 47
C.5 Hosting, Datenbank, Versand, Analyse, Code-Hosting 50
C.6 E-Mail, Office, Speicher, Zusammenarbeit – die leicht übersehenen Kandidaten 56
C.7 Bordmittel von macOS und iOS 60
C.8 Verwaltung, Buchhaltung, Post, Signatur 62
C.9 Wo dieser Anhang weiße Flecken hat 64

TEIL D – DIE DOKUMENTE UND RAHMENBEDINGUNGEN, DIE ICH GEBRAUCHT HABE 65

TEIL E – LEXIKON 68

TEIL F – QUELLEN 73

BEVOR SIE WEITERLESEN – SECHS SÄTZE, DIE ICH ERNST MEINE

1. **Das ist ein Erfahrungsbericht, keine Rechtsberatung.** Ich baue digitale Produkte und begleite Unternehmen; Jurist bin ich nicht. Ich schildere, was ich in meiner eigenen Firma geprüft und entschieden habe, und nenne die Fundstellen, an denen ich es festgemacht habe. Ob etwas in Ihrem Betrieb mit Ihren Daten zulässig ist, ist eine Einzelfallprüfung – die kann dieser Text nicht leisten und darf er auch nicht (§ 2 Abs. 1, § 3 RDG; die allgemeine Darstellung von Rechtsfragen ist nach § 2 Abs. 3 Nr. 5 RDG erlaubt, die Einzelfallprüfung nicht).
2. **Jede Aussage über einen Anbieter stimmt am Tag ihrer Messung – und danach nie wieder garantiert.** Alle Vertragstexte, Tarife und Einstellungen habe ich für dieses Whitepaper am Original gelesen, das Abrufdatum steht jeweils dabei; wo ich das nicht konnte, steht „nicht gemessen“. Anbieter ändern Bedingungen ohne Vorwarnung. Prüfen Sie den Anbietertext des Tages, nicht meine Abschrift.
3. **Der Anhang ist nicht vollständig und will es nicht sein.** Er deckt die Werkzeuge, die ich selbst benutze oder geprüft habe, und je Kategorie die gängigen Alternativen. Ein Werkzeug, das nicht vorkommt, ist damit weder gut noch schlecht – es ist nicht gemessen. Eine Gewähr für Vollständigkeit und für Änderungen nach dem Messtag übernehme ich nicht.
4. **Ich habe eine Präferenz, und ich sage sie.** Ich arbeite überwiegend mit Claude von Anthropic. Das färbt die Beispiele, nicht die Maßstäbe: Die Trennlinie, um die es hier geht, verläuft bei allen großen Anbietern, die ich geprüft habe, im Kern gleich, und der Anhang behandelt sie gleich. Bezahlt werde ich von keinem der genannten Unternehmen.
5. **Für wen das geschrieben ist.** Für Betriebe ohne eigene Rechts- und IT-Abteilung – Selbständige, Berater, Agenturen, kleine Softwarehäuser, grob bis zu einigen Dutzend Beschäftigten. Ab dieser Größe gibt es in der Regel einen Datenschutzbeauftragten (in Deutschland Pflicht, sobald mindestens zwanzig Personen ständig mit automatisierter Verarbeitung befasst sind, § 38 BDSG), und der Text wird zur Prüfliste für ihn statt zur Anleitung für den Inhaber. Konzerne brauchen ihn nicht.

6. **Dieser Text ist mit KI entstanden.** Recherche, Gliederung und Formulierung im Dialog mit Claude (Anthropic); gelesen, korrigiert, entschieden und verantwortet von mir. Eine Kennzeichnungspflicht nach Art. 50 Abs. 4 KI-VO besteht dafür nicht, weil ein Mensch ihn inhaltlich geprüft hat und die Verantwortung trägt – bei diesem Thema wäre es trotzdem seltsam, es nicht zu sagen.

KURZFASSUNG

Die Frage, mit der alles begann, war klein: Darf ich ein KI-Werkzeug mein geschäftliches Postfach lesen lassen? Die Antwort war groß, und sie hatte mit dem Postfach wenig zu tun.

Der Befund: Das Abonnement, mit dem ich seit Monaten gearbeitet hatte – ein Verbrauchertarif, bezahlt von der Firma –, verbietet in seiner Fassung für den Europäischen Wirtschaftsraum die geschäftliche Nutzung ausdrücklich. Es enthält keinen Auftragsverarbeitungsvertrag. Es kann keinen enthalten, weil es für Verbraucher geschrieben ist. Ich hatte in den falschen Kategorien gedacht: „Cloud“ oder „lokal“, „Entwicklung“ oder „Betrieb“. Die Anbieter ziehen die Grenze woanders. Bei allen großen Anbietern, die ich geprüft habe, trennt der Vertrag im Kern zwischen **Verbraucherprodukt und kommerziellem Produkt** – und zwar bei gleicher Oberfläche, gleicher Software, gleichem Anbieter.

Warum das kaum jemand weiß: Die Klausel steht im Haftungskapitel, nicht im Nutzungskapitel. Und dieselbe Internetadresse liefert je nach Standort des Lesers einen anderen Vertragstext – die US-Fassung trägt den Satz nicht.

Was daraus wurde: eine Liste, die länger wurde, nicht kürzer. Der Hoster meiner Website im Gratistarif, der gewerbliche Nutzung ausschließt. Ein Datenbankdienst, dessen Vertragspartner in Singapur sitzt, während die Daten in Frankfurt liegen. Ein Reverse Proxy, der jeden Besucher sieht. Widerspruchsfristen gegen neue Unterauftragnehmer von fünf, sieben, zehn, vierzehn, fünfzehn und dreißig Tagen – die alle nur laufen, wenn man die Benachrichtigung abonniert hat.

Was ich daraus gelernt habe, steht in Teil B als Methode, nicht als Ratschlag: am Anbietertext des Tages messen, Herkunft mitschreiben, aus einem Ausschluss keinen Befund machen, Anzeigen nicht als Messung nehmen, den eigenen Fehler datiert in die Akte schreiben. Und ein Satz, der mir mehr geholfen hat als jede Checkliste: **Kenntnis macht es besser, nicht schlechter – solange auf sie etwas folgt.**

Teil C ist der datierte Werkzeug-Anhang, Teil D die Liste der Dokumente, die ich brauchte, Teil E ein Lexikon der Begriffe, die mir dabei begegnet sind.

TEIL A

DER VORGANG

01 Wie es anfing

02 Der Befund

03 Warum ein Schalter im Konto kein Vertrag ist

04 Die Liste wurde länger, nicht kürzer

05 Die Tarifentscheidung – und was sich dabei nicht messen ließ

06 Was die Preisliste nicht zeigt

01

WIE ES ANFING

Ich baue digitale Produkte, investiere in Gründer und begleite Teams, seit gut dreißig Jahren im Digitalgeschäft und seit 2015 in meiner eigenen Werkstatt, der Wawayaro GmbH in Berlin. Mit KI arbeite ich seit 2023: zuerst ChatGPT im bezahlten Abo, seit Anfang 2026 Claude. Ein großer Teil meiner täglichen Arbeit läuft heute darüber: Schreiben, Programmieren, Belege sortieren, Verträge durcharbeiten, ein Softwareprodukt bauen. Wenn die Werkstatt ein Betriebssystem hat, dann ist es KI. Ich nenne es wawaOS.

Zuerst ein Wort zu meiner Arbeitsweise, weil sie in diesem Text immer wieder vorkommt: Ich habe mich für eine Lösung nach dem Prinzip „so viel wie möglich lokal, so wenig wie nötig in der Cloud“ entschieden. In dieser Lösung liegen meine Datenablage und meine Akten zu allen möglichen Themen und Vorgängen, auch zu meinen Werkzeugen. Eine Akte ist eine laufende Sammlung datierter Vermerke, die meine KI-Umgebung mit mir zusammen pflegt: was ich wann gelesen habe, wo es steht, woher eine Angabe stammt – selbst gelesen, gemessen oder nur gehört – und was daraus folgte, bis hin zu offenen Punkten mit Termin. So behalte ich die Kontrolle über meine Daten, und jede Entscheidung und jeder Arbeitsschritt lässt sich im Nachhinein lückenlos nachvollziehen. Nebenbei erspart es mir, dieselbe Frage dreimal zu prüfen. Diese Akte ist die Quelle dieses Textes.

Über den Rechtsrahmen habe ich früh geschrieben – im Mai 2023 auf LinkedIn zu ChatGPT im deutschen Rechtsrahmen, kurz darauf einen Wegweiser zu KI in Deutschland und der EU, im Juni 2023 zum damals noch verhandelten AI Act. Ich hielt mich also für jemanden, der das sorgfältig macht: Training in den Einstellungen abgeschaltet, keine Passwörter in Prompts, Produktivdaten meines Softwareprodukts laufen ausschließlich über die Programmierschnittstelle (API) mit Geschäftsvertrag – also nie über die Chat-Oberfläche.

Dann wollte ich einen Schritt weiter: Das Werkzeug sollte mein geschäftliches Postfach maschinell mitlesen. Das Postfach ist ein Sammelpostfach – dort kommen Nachrichten Dritter an, mit Namen, Anliegen, Anhängen. Ich wusste, dass das eine datenschutzrechtliche Frage ist, und habe sie vor dem ersten Klick geprüft.

Ich habe damit gerechnet, einen Auftragsverarbeitungsvertrag abschließen zu müssen – den Vertrag, den die Datenschutz-Grundverordnung verlangt, wenn ein Dienstleister personenbezogene Daten für mich verarbeitet (Art. 28 DSGVO). Ich habe nicht damit gerechnet, dass es keinen gibt.

02

DER BEFUND

Mein Abonnement war Claude Max 20x – damals der teuerste Verbrauchertarif von Anthropic, bezahlt von der Firma, aber ein Verbrauchertarif. Ich habe die Nutzungsbedingungen gelesen, die für Verbraucher im Europäischen Wirtschaftsraum gelten. Dort steht, in Abschnitt 11, unter der Überschrift der Haftungsbeschränkungen:

> „Non-commercial use only. You agree that you will not use our Services for any commercial or business purposes …“
>
> Anthropic, Consumer Terms of Service (EWR und Schweiz), Abschn. 11 · abgerufen 27.11.2026

Und gleich zu Beginn, wer überhaupt gemeint ist:

> „These Terms apply to you if you are a consumer who is resident in the European Economic Area or Switzerland. You are a consumer if you are acting wholly or mainly outside your trade, business, craft or profession in using our Services.“
>
> Anthropic, Consumer Terms of Service (EWR und Schweiz), Geltungsbereich · abgerufen 27.11.2026

(Anthropic, Consumer Terms of Service, Fassung für EWR und Schweiz, wirksam 08.10.2025; für dieses Whitepaper am 27.11.2026 aus einer EU-Umgebung abgerufen, Textauszug als Beleg gesichert. Vertragspartnerin dieser Fassung ist Anthropic Ireland, Limited.)

Damit hing der Verstoß nicht mehr an der Frage, ob personenbezogene Daten im Spiel sind. Er hing schon an der geschäftlichen Nutzung selbst. Das ist einfacher als Art. 28 DSGVO – und härter.

Bei OpenAI sind die Verbrauchertarife im Kern ähnlich gebaut: kein Auftragsverarbeitungsvertrag, Training nur als Einstellung abschaltbar. **Geschäftliche Nutzung und Automatik regelt OpenAI dagegen großzügiger als Anthropic.**

Drei Dinge habe ich daran gelernt, und keines davon steht in einem Ratgeber:

Erstens: Die Klausel steht dort, wo niemand nach ihr sucht. Wer wissen will, was er darf, liest das Nutzungskapitel. Der Satz steht im Haftungskapitel, als Begründung dafür, dass der Anbieter für entgangenen Gewinn und Betriebsunterbre-

chung nicht haftet – bei Verbrauchern, so meine Lesart, gibt es keinen Geschäftsgewinn, der entgehen könnte. Die Logik ist schlüssig. Sie steht nur nicht dort, wo man sie erwartet.

Zweitens: Dieselbe Adresse liefert nicht denselben Text. Ruft man dieselbe Seite aus einer US-Umgebung ab, kommt eine andere Fassung: Vertragspartnerin Anthropic, PBC in den USA, kalifornisches Recht, und der Satz zur ausschließlich nichtgeschäftlichen Nutzung fehlt. Die englischsprachige Debatte im Netz dreht sich erkennbar um diesen anderen Text. Wer in einem Forum liest „das kann nicht stimmen, sonst würden alle, die ich kenne, gegen die Bedingungen verstoßen", liest die Antwort eines Menschen, der eine andere Fassung vor sich hat. Beide haben recht – jeder für seinen Kontinent.

Drittens: Verbreitung ist kein Rechtfertigungsgrund. Der Reflex, der sofort kommt, heißt: „Aber das machen doch alle." Stimmt. Es „machen" auch alle ihren Mailverkehr über ein kostenloses Postfach eines großen Anbieters. Wer das rechtskonform tut, nutzt die Geschäftsvariante mit Auftragsverarbeitungsvertrag. Wer ein kostenloses Verbraucherpostfach für Kundenverkehr nutzt, hat dafür keinen Auftragsverarbeitungsvertrag – obwohl der Anbieter die Kundendaten in seinem Auftrag verarbeitet, und genau dafür verlangt Art. 28 DSGVO einen. Es fällt nur nie auf.

03

WARUM EIN SCHALTER IM KONTO KEIN VERTRAG IST

Mein zweiter Irrtum war bequemer als der erste. Ich hatte das Training in den Kontoeinstellungen abgeschaltet und hielt die Sache damit für geregelt. Zwei Gründe, warum das nicht trägt:

1. Eine Einstellung ist einseitig änderbar und beweist im Streitfall nichts. Ein **vertraglicher** Trainingsausschluss steht im Geschäftsvertrag und ist einklagbar. Die kommerziellen Bedingungen desselben Anbieters formulieren es als Zusage: „Anthropic may not train models on Customer Content from Services." Das ist ein Versprechen, keine Option.
2. Die Einstellung sagt nichts über die **Speicherdauer**. Auf der Verbraucherseite verlängert die Zustimmung zum Training die Aufbewahrung erheblich; wer sie abschaltet, verkürzt sie – aber auch das ist eine Produktbeschreibung, kein Vertragsinhalt.

Für meinen eigenen Kundenvertrag ist das nicht nebensächlich: Die Auftragsbedingungen, die ich mit jedem Beratungsmandat vereinbare, sagen meinen Kunden zu, dass ich nur Werkzeuge mit vertraglichem Trainingsausschluss verwende. Ein Häkchen in einem Verbraucherkonto erfüllt diese Zusage nicht. Ich hätte meinen Kunden etwas versprochen, was ich mit dem gewählten Tarif gar nicht halten konnte. Wer Software baut oder eine Agentur führt, hat dieselbe Zusage meist an anderer Stelle gegeben: im Entwicklungs- oder Wartungsvertrag oder im Auftragsverarbeitungsvertrag mit dem eigenen Kunden.

04

DIE LISTE WURDE LÄNGER, NICHT KÜRZER

Wer einmal anfängt, am Vertragstext zu messen statt an dem, was man über einen Dienst zu wissen glaubt, hört nicht beim ersten Werkzeug auf. Was ich in den folgenden Tagen gefunden habe – alles am Anbietertext des jeweiligen Tages gelesen, Fundstellen im Anhang:

Der Hoster meiner Website lief im Gratistarif eines bekannten Anbieters (Vercel, Tarif „Hobby"). Der Tarif ist laut Anbieter „restricted to non-commercial personal use only", und der Auftragsverarbeitungsvertrag des Anbieters gilt ausdrücklich nur für die Tarife Pro und Enterprise. Eine Firmenwebsite mit Kontaktformular auf diesem Tarif: zwei Befunde in einem Zug. Der Weg heraus ist entweder der bezahlte Tarif oder ein anderer Hoster – ich bin zu einem deutschen Anbieter umgezogen, den ich für andere Zwecke ohnehin bezahle. Wer vor derselben Frage steht, findet im Anhang die üblichen Alternativen (Vercel Pro, Netlify, netcup, Hetzner, IONOS, Strato) mit dem jeweiligen Weg zum Vertrag.

Der Datenbankdienst meines Softwareprodukts (Supabase) hatte den Vertrag längst – er gilt automatisch mit Annahme der Nutzungsbedingungen, samt Standardvertragsklauseln. Das war die gute Nachricht. Die weniger gute: Vertragspartnerin ist eine Gesellschaft in Singapur, also in einem Drittland ohne Angemessenheitsbeschluss – obwohl die Daten in Frankfurt liegen, weil ich beim Anlegen bewusst eine EU-Region gewählt habe. „EU-Hosting" und „EU-Vertragspartner" sind zwei verschiedene Dinge, und die Drittlandfrage stellt sich auch für Daten, die Europa nie verlassen. Zweite Beobachtung: Der Dienst darf nach seinem Vertrag überall verarbeiten, wo er Einrichtungen unterhält, solange der Kunde keine Region vorgibt. Die Region ist also keine Voreinstellung, sondern eine Entscheidung – wer sie nicht trifft, hat sie getroffen.

Der Reverse Proxy vor beiden Domains (Cloudflare) – der Dienst, durch den jeder Aufruf einer Website läuft, bevor er den eigentlichen Server erreicht – sieht jede IP-Adresse und jeden Request. In meiner Übersicht der Dienste stand er als „DNS und Captcha". Das unterschätzt ihn um Größenordnungen. Der Vertrag gilt hier immerhin auch im Gratistarif automatisch – aber in Datenschutzerklärung und Verarbeitungsverzeichnis muss er stehen, und dort stand er nicht.

Die Widerspruchsfristen. Fast jeder Dienst setzt seinerseits Dienstleister ein – Rechenzentren, Support, Zahlungsabwickler; im Vertrag heißen sie Unterauftragsverarbeiter. Kommt ein neuer hinzu, darf der Kunde widersprechen. Bei den Anbietern, die ich geprüft habe, hat man dafür fünf Tage (Supabase), sieben Tage (Postmark), zehn Tage (Cloudflare, Mistral, Railway), vierzehn Tage (Resend), fünfzehn Tage (Anthropic) oder dreißig Tage (OpenAI). Alle diese Fristen haben eines gemeinsam: Sie laufen ab Mitteilung – und die Mitteilung bekommt nur, wer sich auf einer Webseite in eine Benachrichtigungsliste eingetragen hat. Wer das nicht getan hat, erfährt von einem neuen Unterauftragnehmer in der Regel nicht – und verpasst damit die Frist, ihm zu widersprechen. Ich hatte es bei keinem einzigen Anbieter getan.

Die technischen und organisatorischen Maßnahmen – das, was ein Anbieter zum Schutz der Daten zusagt: Verschlüsselung, Zugriffskontrolle, Backups. Bei einem der geprüften Anbieter sind diese Maßnahmen ausdrücklich nicht Vertragsbestandteil, sondern eine Beschreibung auf einer Unterseite. Bei den anderen sind sie ein Anhang des Vertrags. Für die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) ist das ein erheblicher Unterschied, und man sieht ihn nur, wenn man den Vertrag liest statt das Werbeblatt.

Die Werkzeuge im eigenen Haus. Buchhaltungssoftware, Postdigitalisierer, Signaturdienst: Bei den deutschen Anbietern ist der Auftragsverarbeitungsvertrag fast immer da – aber er wird meist nicht automatisch mitgeliefert, sondern muss erst durch Klick angefordert bzw. abgeschlossen werden. Ich hatte das bei einem Teil getan und beim anderen nicht, und ich konnte aus dem Gedächtnis nicht sagen, bei welchem.

05

DIE TARIFENTSCHEIDUNG – UND WAS SICH DABEI NICHT MESSEN LIESS

Der naheliegende Weg aus dem Befund heißt: Wechsel auf das kommerzielle Produkt desselben Anbieters – bei Anthropic von Claude Max auf Claude Team oder Enterprise. Dort gilt der Auftragsverarbeitungsvertrag automatisch, dort steht der Trainingsausschluss im Vertrag, dort ist die Vertragspartnerin eine irische Gesellschaft. Ich hatte drei Einwände, und alle drei hielten der Messung nicht stand.

„Der Team-Tarif ist für ein einzelnes Konto zu teuer." Der Team-Tarif verlangt mindestens zwei Sitze. Ich hatte im Kopf: zwei Premium-Sitze, doppelter Preis. Gemessen am Listenpreis (claude.com/pricing, abgerufen 27.11.2026: Premium-Sitz 125 USD, Standard-Sitz 25 USD, jeweils monatlich) ist die richtige Bestellung ein Premium-Sitz plus ein Standard-Sitz – und die kostet nach Liste weniger, als ich bisher für das große Verbraucherabo bezahlt hatte. Der Preis liegt woanders: Nach der Preisseite bietet der Premium-Sitz das Fünffache eines Standard-Sitzes, mein bisheriges Verbraucherabo bot das Zwanzigfache von Pro – der Premium-Sitz bringt also ein kleineres Kontingent. Was fehlt, kauft man über Nutzungsguthaben zu den regulären Schnittstellenpreisen nach („billed at standard API rates", Anthropic-Hilfeartikel 12005970, abgerufen 27.11.2026) – ohne Aufschlag, aber auch ohne den Mengenrabatt, den das Verbraucherabo enthält. Dazu kommt eine Umstellung, die man vorher kennen sollte: Zum Team-Tarif gehört ein monatliches Guthaben für die Programmierschnittstelle (laut Preisseite bis zu 500 USD im Monat, für die Organisation zusammengefasst, abgerufen 28.11.2026). Es wird genutzt wie die Schnittstelle selbst, und was im Monat nicht verbraucht ist, verfällt. Wer bisher ausschließlich im Chat gearbeitet hat, muss also lernen, mit einem Monatsbudget zu planen – und unter Umständen die eigene Arbeitsweise anpassen, damit es sinnvoll eingesetzt wird.

„Nachgekauftes Guthaben ist eine Kostenfalle." Die Sorge: Was über den Sitz hinausgeht, wird zu Schnittstellenpreisen abgerechnet, und die Rechnung läuft unbemerkt hoch. Die kommerziellen Produkte lassen dafür Ausgabengrenzen set-

zen, für die ganze Organisation und je Nutzer (claude.com/pricing: Ausgabengrenzen im Team-Tarif, abgerufen 27.11.2026). Mit einer gesetzten Grenze ist die Höhe der Rechnung eine Entscheidung, keine Überraschung.

„Ich weiß nicht, wie viel ich eigentlich verbrauche." Das war der Einwand, der blieb. Der Bildschirm im Konto, der den Verbrauch anzeigt („Einstellungen › Nutzung"), zeigt keine absoluten Werte, sondern Prozentsätze einer nicht genannten Bezugsgröße, verteilt auf drei ineinandergeschobene Zeitfenster – und die Bezugsgröße bewegt sich: Während meiner Prüfung lief eine zeitlich begrenzte Erhöhung der Limits (Hinweisband im Nutzungsbildschirm, eigene Beobachtung), die den angezeigten Prozentsatz senkt, ohne dass sich mein Verhalten geändert hätte. Ein Bildschirm, der Prozent von etwas zeigt, das sich durch Aktionen des Anbieters verschiebt, kann keine Kaufentscheidung tragen.

Auch ein zweiter Weg, den Bedarf zu schätzen, trug nicht: Ich wollte ihn an meinen bisherigen Nachkäufen von Zusatzkontingent ablesen. Doch ein vorhandenes Guthaben war zuerst verrechnet worden, es gab also keine Zahlungen, an denen sich etwas ablesen ließ. Das belegte fehlende Zahlungen, nicht fehlenden Bedarf. Ich hatte den Vorbehalt „ein Ausschluss belegt nur den Ausschluss" sogar in meiner eigenen Notiz stehen – und ihn trotzdem übergangen.

Ergebnis: Der Bedarf ist aus meiner Akte nicht messbar. Er wird nach dem Wechsel an der ersten Abrechnung gemessen, nicht vorher hergeleitet. Die Entscheidung für das kommerzielle Produkt hängt davon nicht ab – sie folgt aus dem Vertragsrecht, nicht aus der Verbrauchsmessung.

Ein letzter Punkt, weil er im Gespräch mit Unternehmern immer kommt: **Muss ich dem Anbieter gegenüber etwas eingestehen?** Nein. Eine Anfrage an den Vertrieb ist vorwärts gerichtet: kleine Gesellschaft, bislang ein einziges Konto, braucht kommerzielle Bedingungen und mehr Kontingent als ein Premium-Sitz – welcher Weg. Über die Vergangenheit wurde nicht gefragt, und in meinem Fall gab es keinen Anlass, sie unaufgefordert zu erzählen. Wird direkt gefragt, wird wahrheitsgemäß geantwortet. Der Vorgang selbst – ein Kunde wechselt auf das kostenpflichtige kommerzielle Produkt – ist genau die Maßnahme, die das Gesetz zugunsten dessen wertet, der einen Mangel abstellt (dazu Teil B, Abschnitt 9). Ich habe die Anfrage gestellt, mir gleichzeitig ein Enddatum gesetzt und dann gewechselt. Ein datierter, begründeter Aufschub ist etwas anderes als ein geduldeter Dauerzustand.

06

WAS DIE PREISLISTE NICHT ZEIGT

Beim Wechsel wandert nicht alles mit. Der Anbieter schreibt in seiner Hilfe zum Wechsel vom Verbraucher- in das Teamkonto, für eigene Erweiterungen gebe es keinen Migrationspfad („There is no migration path for skills. Export any you want to keep before you migrate.“, abgerufen 27.11.2026), verbundene Anwendungen verlören ihre Autorisierung, selbst angelegte Verbindungen müssten neu erstellt werden. Wer monatelang eine Arbeitsumgebung gebaut hat, zieht sie nicht um – er baut sie neu. Das ist kein Argument gegen den Wechsel. Es ist ein Posten auf der Rechnung, den die Preisliste nicht zeigt. In der Praxis war der Umstieg trotzdem recht problemlos, solange man die Anleitung des Anbieters Schritt für Schritt befolgt.

WAS BEIM WECHSEL NICHT MITZIEHT

- Eigene Erweiterungen (Skills): kein Migrationspfad, vorher exportieren
- Verbundene Anwendungen verlieren ihre Autorisierung
- Selbst angelegte Verbindungen müssen neu erstellt werden

Und noch etwas gehört hierher, weil es sonst niemand schreibt: **Ein Befund ist erst erledigt, wenn er umgesetzt ist.** Der Tarifwechsel, der Hosterwechsel und das Abonnement der Benachrichtigungen standen jeweils mit Datum, Grund und Termin in der Akte, bis sie umgesetzt waren. Ein Text, der so tut, als sei mit dem Befund schon alles sauber, wäre genau der Ratgeber, der ich nicht sein will.

Rechtssicherheit ist kein Zustand, den man einkauft. Sie ist eine Kette von Entscheidungen, bei der jede Lösung eine neue Frage aufmacht. Wer das weiß, arbeitet anders als wer es nicht weiß – nicht ängstlicher, sondern mit Akte.

Rechtssicherheit ist kein Zustand, den man einkauft.

TEIL B

WAS ICH DARAUS GELERNT HABE

Dieser Teil ist so geschrieben, dass er in einem Jahr noch stimmt. Er nennt keine Preise und keine Tarifnamen – die stehen im datierten Anhang. Er nennt Maßstäbe.

01 Die Trennlinie, an der sich alles entscheidet

02 Drei Achsen – und eine, die keine ist

03 Die fünf Nebenwege – der eigentliche Regelungsbedarf

04 Was am Auftragsverarbeitungsvertrag tatsächlich zu prüfen ist

05 EU-Hosting, EU-Vertragspartner, EU-Verarbeitung – drei Dinge, nicht eines

06 Was heute gilt – der Rechtsrahmen in einer Seite

07 Was eine Datenschutzerklärung nicht heilt

08 Kenntnis macht es besser, nicht schlechter

09 Die Methode – sechs Regeln, die ich seither anwende

10 So bin ich vorgegangen – zehn Fragen, die ich mir je Werkzeug gestellt habe

01

DIE TRENNLINIE, AN DER SICH ALLES ENTSCHEIDET

Nicht Entwicklung gegen Betrieb. Nicht Cloud gegen lokal. Nicht Anbieter A gegen Anbieter B. Sondern: **Verbraucherprodukt gegen kommerzielles Produkt – beim selben Anbieter, mit derselben Oberfläche.**

	Verbrauchertarif	Kommerzielles Produkt
Vertragswerk	Consumer Terms / Nutzungsbedingungen für Privatkunden	Commercial Terms / Business Terms / Services Agreement
Geschäftliche Nutzung	je nach Anbieter verboten, geduldet oder mit Zusatzklauseln – nie das vorgesehene Produkt	der Vertragszweck
Auftragsverarbeitungsvertrag (Art. 28 DSGVO)	**existiert nicht**	Bestandteil – gilt mit Annahme oder ist per Selbstbedienung abzuschließen
Trainingsausschluss	Produkteinstellung im Konto, einseitig änderbar	**vertragliche Zusage**
Drittlandgrundlage	Datenschutzerklärung des Anbieters	Standardvertragsklauseln und/oder DPF-Zertifizierung im Vertrag
Vertragspartner (EWR)	je nach Anbieter US-Gesellschaft oder EU-Tochter	in der Regel EU-Tochter, EU-Recht
Speicherdauer, Löschung, Meldefristen	Produktbeschreibung	Vertragsinhalt

GLEICHE OBERFLÄCHE, ANDERER VERTRAG

Verbraucher- und Geschäftstarif beim selben Anbieter

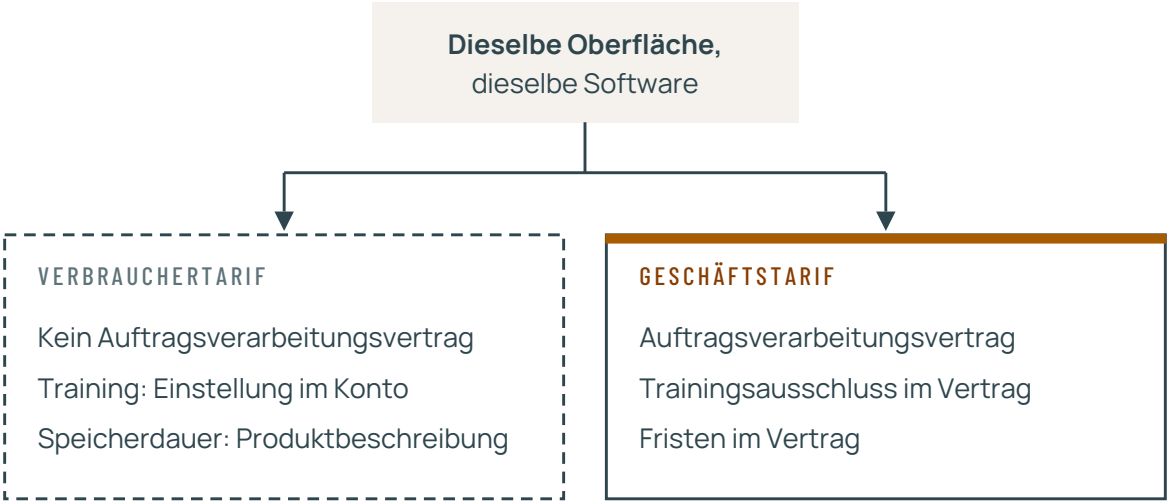

ABB. 1 · Was den Unterschied macht, steht nicht in der Software, sondern im Vertrag.
Eigene Darstellung

Der Satz, der das zusammenfasst und den ich seither in jedem Gespräch sage: **Anbieten ist nicht Erlauben.** Dass ein Werkzeug einen Postfach-Connector, einen Datei-Upload oder eine Kalenderanbindung anbietet, sagt nichts darüber, ob man ihn im gewählten Tarif rechtmäßig für Kundendaten benutzen darf. Die Funktion ist dieselbe. Der Vertrag nicht.

Anbieten ist nicht Erlauben.

02

DREI ACHSEN – UND EINE, DIE KEINE IST

Ich hatte lange in „Entwicklung oder Betrieb“ gedacht: Im Betrieb fließen Kundendaten, in der Entwicklung Quelltext, also ist die Entwicklung unkritisch. Das ist ein guter Indikator und kein Maßstab. Die Datenschutz-Grundverordnung kennt keine Entwicklungsausnahme – nach Art. 4 Nr. 2 ist jeder Vorgang mit personenbezogenen Daten eine Verarbeitung, gleich ob in einer Testumgebung oder in Produktion.

Was die Lage bestimmt, sind drei Fragen, die in der Praxis ständig zusammengeworfen werden:

Achse	Frage	Was davon abhängt
Produkt	Kommerzieller Tarif oder Verbraucherabo?	ob überhaupt ein Auftragsverarbeitungsvertrag existiert
Rolle	Wessen Daten – und bin ich dafür Verantwortlicher?	ob Art. 28 DSGVO greift
Inhalt	Sind im Datenstrom überhaupt Personendaten?	ob die DSGVO anwendbar ist

„Entwicklung oder Betrieb“ kommt in keiner der drei vor. Entwicklungsarbeit ist meistens unkritisch – nicht weil sie Entwicklung ist, sondern weil Quelltext, Schemata, Konzepte und synthetische Testdaten schlicht keine Personendaten sind.

Zwei Einschränkungen, die dabei regelmäßig übersehen werden: **Pseudonymisierung genügt nicht** – pseudonymisierte Daten bleiben personenbezogen (Art. 4 Nr. 5); nur echte Anonymisierung führt aus dem Anwendungsbereich heraus, und ein Datensatz mit ersetzten Namen, aber stehen gebliebenen Adressen, Datumsangaben und Freitexten ist nicht anonym. Und **Datenschutz ist nicht der einzige Maßstab**: Quelltext und Kundenmaterial sind auch ohne Personenbezug schutzbedürftig – als Geschäftsgeheimnis (§ 2 GeschGehG setzt angemessene Geheimhaltungsmaßnahmen voraus; wer Kalkulationen in ein Werkzeug mit Trainingsrecht gibt, gefährdet sie), aus Vertraulichkeitsklauseln und aus jeder Geheimhaltungsvereinbarung mit einem Kunden.

03

DIE FÜNF NEBENWEGE – DER EIGENTLICHE REGELUNGSBEDARF

Ein sauber gebauter Produktivpfad über die Programmierschnittstelle mit Geschäftsvertrag schützt vor keinem der Wege, auf denen fremde Personendaten tatsächlich in ein Verbraucherwerkzeug geraten. Diese Wege umgehen die Architektur vollständig und fallen deshalb in keiner Architekturprüfung auf. Bei mir waren es fünf:

1. ein **Datenbankauszug** zur Fehlersuche, in den Chat kopiert
2. ein **Logauszug** mit IP-Adressen, E-Mail-Adressen oder Sitzungskennungen
3. ein **Screenshot** eines Dashboards oder einer Gesprächsoberfläche mit echten Inhalten
4. ein **Supportfall**, den man „mal eben“ schildert, samt Kundenname
5. ein **Testdatensatz**, der aus Produktion gezogen wurde, weil synthetische Daten den Fehler nicht reproduzieren – zusätzlich eine Zweckänderung nach Art. 6 Abs. 4 DSGVO

FÜNF NEBENWEGE UMGEHEN DEN SAUBEREN PFAD

Wie Kundendaten aus dem eigenen Betrieb in ein Verbraucherwerkzeug gelangen



ABB. 2 · Keiner dieser Wege berührt die Architektur – deshalb fällt keiner in einer Architekturprüfung auf. Eigene Darstellung

Die Frage ist also nicht, ob im Betrieb Kundendaten in das Verbraucherwerkzeug gelangen. Die Frage ist, ob sie es in der Entwicklung tun. **Das ist der eigentliche Regelungsbedarf, und er kostet nichts – es ist eine Werkzeugregel, kein Tarif.** Die Regel, die daraus folgt, ist ein Satz: Kein Weg führt von Produktivdaten in ein Verbraucherwerkzeug; wo ein Fehler ohne echte Daten nicht reproduzierbar ist, wird der Datensatz vorher anonymisiert – nicht pseudonymisiert.

04

WAS AM AUFTRAGSVERARBEITUNGSVERTRAG TATSÄCHLICH ZU PRÜFEN IST

Nicht „gibt es einen“, sondern **was drinsteht**. Acht Prüfpunkte, aus meiner eigenen Durchsicht, in der Reihenfolge, in der sie mich überrascht haben:

Prüfpunkt	Warum er zählt
Geltungsweg	Gilt der Vertrag automatisch mit den Nutzungsbedingungen, ist er per Klick im Kundenportal abzuschließen, oder wird er erst mit Gegenzeichnung des Anbieters wirksam? Alle drei kommen vor – und beim dritten liegt zwischen Kontoeröffnung und Unterschrift eine Lücke
Für welche Tarife	Manche Verträge gelten wörtlich nur für bezahlte Pläne. Der Gratistarif ist dann vertragslos, auch wenn der Vertrag auf der Website steht
Vertragspartner	EU-Gesellschaft oder Drittland? Entscheidet über Recht, Gerichtsstand und Aufwand im Ernstfall – und er kann innerhalb desselben Anbieters mit dem Tarif wechseln
Drittlandgrundlage	Standardvertragsklauseln (welches Modul), DPF-Zertifizierung, UK- und Schweiz-Zusatz. „Server in Frankfurt“ ist keine Drittlandgrundlage, wenn der Vertragspartner in Singapur sitzt
Meldefrist bei Sicherheitsvorfall	Die 72 Stunden aus Art. 33 DSGVO laufen gegen mich. Ein Auftragsverarbeiter, der 48 Stunden zusagt, lässt Puffer; einer, der „unverzüglich“ sagt, lässt keinen
Widerspruchsfrist bei Unterauftragsverarbeitern	**Der am meisten unterschätzte Punkt.** Fünf bis dreißig Tage, ab Mitteilung – und die Mitteilung gibt es nur nach Anmeldung
Sind die technischen und organisatorischen Maßnahmen Vertragsbestandteil	Anhang des Vertrags oder Beschreibung auf einer Unterseite? Für die Rechenschaftspflicht ein erheblicher Unterschied
Löschung nach Vertragsende, einseitiges Änderungsrecht	Frist, Rückgabeanspruch, Ausnahmen; Schweigen als Zustimmung zu Änderungen ist üblich – man sollte es wissen

Der Befund, der sich am besten zum Weitererzählen eignet, weil er ein Muster zeigt und nicht einen Anbieter: **Acht geprüfte Anbieter, sechs verschiedene Widerspruchsfristen – fünf, sieben, zehn, vierzehn, fünfzehn und dreißig Tage.**

ACHT ANBIETER, SECHS VERSCHIEDENE FRISTEN

Zeit für einen Widerspruch gegen neue Unterauftragsverarbeiter, in Tagen ab Mitteilung

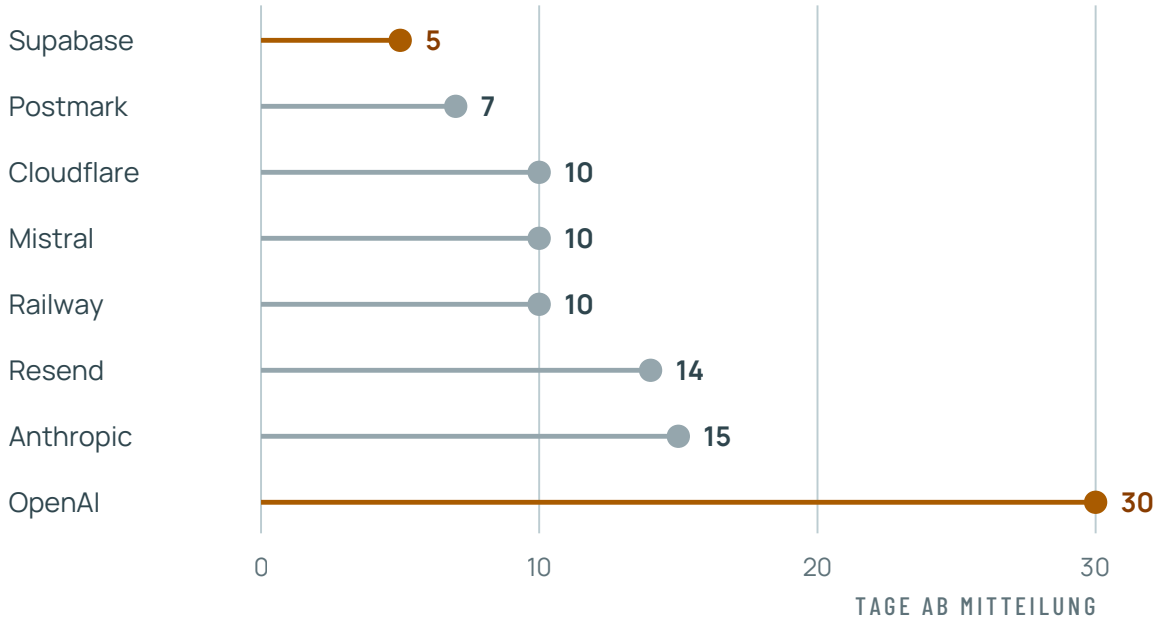

ABB. 3 · Jede Frist läuft ab Mitteilung – die erhält nur, wer sich in die Benachrichtigungsliste des Anbieters eingetragen hat. Hervorgehoben: kürzeste und längste Frist.

Quelle: AVV der Anbieter, abgerufen 27.11.2026

Was ein Widerspruch bewirkt, regelt jeder Vertrag selbst. Art. 28 Abs. 2 DSGVO verlangt nur, dass man vor dem Einsatz eines neuen Unterauftragsverarbeiters informiert wird und Einspruch erheben kann. In den Verträgen, die ich gelesen habe, läuft ein Widerspruch im Kern auf zwei Wege hinaus: Man klärt den Einwand mit dem Anbieter, oder man kündigt den betroffenen Dienst. Wer nicht widerspricht – bewusst oder weil die Mitteilung nie ankam –, bei dem setzt der Anbieter den neuen Dienstleister nach Fristablauf ein; die allgemeine Genehmigung im Vertrag deckt das. Meist ist das kein Drama. Heikel wird es, wenn der Neue in einem Drittland sitzt oder wenn man den eigenen Kunden zugesagt hat, nur bestimmte Dienstleister einzusetzen.

05

EU-HOSTING, EU-VERTRAGSPARTNER, EU-VERARBEITUNG – DREI DINGE, NICHT EINES

„Die Daten liegen in Europa“ ist der Satz, mit dem jede Anbieterseite wirbt, und er beantwortet nur eine von drei Fragen.

- **Wo liegen die Daten?** (Datenresidenz) – Frankfurt, Irland, Nürnberg. Bei vielen Diensten frei wählbar, aber meist nur beim Anlegen; ein Wechsel ist eine Migration.
- **Mit wem habe ich den Vertrag?** (Vertragspartner) – eine irische Tochter, eine Gesellschaft in Singapur, eine in Delaware. Bestimmt Recht, Gerichtsstand und ob überhaupt eine Drittlandübermittlung vorliegt.
- **Wo wird gerechnet, und wer greift zu?** (Verarbeitungsort) – Bei KI-Modellen ist die Inferenz oft nur in den USA oder „global“ verfügbar, auch wenn der Vertragspartner in Dublin sitzt; Missbrauchskontrolle und Support können aus Drittländern zugreifen; bei mindestens einem großen Anbieter kann die Inferenz bei Lastspitzen standardmäßig aus der EU-Datengrenze herauswandern, wenn der Administrator es nicht abschaltet (laut Anbieter-Mitteilung, sekundär belegt).

„IN DER EU" BEANTWORTET NUR EINE VON DREI FRAGEN

Drei Fragen hinter „Daten in Europa", Beispiel Datenbankdienst aus Teil A

FRAGE	BEISPIEL DATENBANKDIENST
Wo liegen die Daten? Datenresidenz	Frankfurt, beim Anlegen gewählt
Mit wem ist der Vertrag? Vertragspartner	**Gesellschaft in Singapur**
Wo wird gerechnet, wer greift zu? Verarbeitungsort	Ohne Regionsvorgabe: überall, wo der Anbieter Einrichtungen hat

ABB. 4 · Die Region beim Anlegen zu wählen, klärt nur den Speicherort. Vertragspartner und Rechenort sind eigene Fragen. Eigene Darstellung

Erst die Kombination senkt den Prüfaufwand wirklich: EU-Vertragspartner, EU-Speicherung, kein oder abgesicherter Zugriff aus Drittländern. Eine EU-Tochter eines US-Konzerns kann zudem über die Muttergesellschaft US-Zugriffsbefugnissen ausgesetzt sein – das ist kein Argument gegen sie, aber ein Grund, es zu wissen.

06

WAS HEUTE GILT – DER RECHTSRAHMEN IN EINER SEITE

Ich fasse zusammen, was ich im Lauf meiner Recherche selbst nachgelesen und für dieses Whitepaper im November 2026 nochmals überprüft habe. Fundstellen im Lexikon und im Quellenverzeichnis.

Die DSGVO ist unverändert. Der von der Kommission vorgeschlagene „Data Omnibus" mit Änderungen an der Verordnung ist noch im Gesetzgebungsverfahren: Der Rat hat seine Verhandlungsposition im Oktober 2026 beschlossen, das Parlament noch nicht, ein Trilog hat nicht begonnen (Stand 27.11.2026, sekundär belegt). Alles, was hier zu Art. 28, Art. 30, Art. 33, Art. 35 und Art. 44 ff. steht, gilt wie seit 2018.

Die KI-Verordnung hat einen neuen Zeitplan. Die Verordnung (EU) 2026/1744 („Digital Omnibus on AI") ist am 27.07.2026 in Kraft getreten. Für ein kleines Unternehmen, das KI-Werkzeuge als **Betreiber** nutzt, gilt heute: die Pflicht, für ausreichende KI-Kompetenz des eigenen Personals Maßnahmen zu ergreifen (Art. 4, seit 02.02.2025, durch den Omnibus abgeschwächt); die Verbote (Art. 5); und seit dem **02.08.2026** die Transparenzpflichten des Art. 50 – für Betreiber vor allem Abs. 4: Wer einen Deepfake erzeugt oder verbreitet, muss das offenlegen, und wer KI-Text zur Information der Öffentlichkeit über Angelegenheiten von öffentlichem Interesse veröffentlicht, ebenfalls – außer ein Mensch hat ihn inhaltlich geprüft – nicht nur Korrektur gelesen – und trägt die redaktionelle Verantwortung. Die Hochrisiko-Pflichten nach Anhang III (Personalauswahl, Bonitätsscoring) gelten erst ab dem 02.12.2027. Für Kundenmails, Angebote und Produkttexte, die nicht der Information der Öffentlichkeit dienen, folgt aus Art. 50 Abs. 4 heute praktisch nichts; ein Kunden-Chatbot muss so gebaut sein, dass der Kunde erkennt, mit einer Maschine zu sprechen – eine Pflicht des Anbieters (Art. 50 Abs. 1), die jeden trifft, der den Chatbot selbst baut.

TIPP · INHALTLICH GEPRÜFT ODER NUR KORREKTUR GELESEN?

Korrektur lesen heißt: Rechtschreibung, Ausdruck, Lesefluss. Inhaltlich prüfen heißt: für die Aussagen einstehen – die Fakten nachsehen, die Quellen lesen, die Schlussfolgerungen selbst ziehen. Meine Faustregel: Könnte ich jeden Satz auf Nachfrage begründen, ohne das Werkzeug zu fragen? Dann habe ich ihn geprüft. Habe ich nur geglättet, was die Maschine geschrieben hat, eher nicht.

Der Betreiber ist nicht der Anbieter. Die Markierungs- und Produktpflichten treffen OpenAI, Anthropic, Google, Microsoft und die anderen. Wer aber ein fremdes Modell unter eigener Marke wesentlich verändert oder ein offenes Modell selbst betreibt und unter eigenem Namen anbietet, kann selbst Anbieter werden (Art. 25) – mit allen Pflichten.

Der Datentransfer in die USA steht auf einem Beschluss, an dem gezogen wird. Das EU-US Data Privacy Framework gilt. Die Klage dagegen hat das Gericht der EU im September 2025 abgewiesen; das Rechtsmittel ist beim EuGH anhängig. Seit dem Sommer 2026 kommt hinzu, dass der US Supreme Court die Unabhängigkeit einer Aufsichtsbehörde eingeschränkt hat, auf die der Beschluss baut (Stand und Tragweite umstritten); Datenschutzverbände und der Europäische Datenschutzausschuss haben die Kommission zur Prüfung aufgefordert. Was ich daraus gemacht habe: Bei jedem US-Anbieter prüfen, ob die Standardvertragsklauseln als Rückfall im Vertrag stehen. Bei den großen tun sie das.

Bei Gesprächen gilt zuerst das Strafrecht, dann der Datenschutz. Wer das nichtöffentlich gesprochene Wort eines anderen ohne dessen Einwilligung aufnimmt, macht sich nach § 201 StGB strafbar – auch wenn die Aufnahme nur der Transkription dient und danach gelöscht wird. Ein Meeting-Assistent nimmt auf; Täter ist der Nutzer, nicht der Anbieter. Der Aufnahmehinweis der Konferenzplattform informiert, er holt keine Einwilligung ein. Und wer für Ärzte, Anwälte oder Steuerberater arbeitet, ist „mitwirkende Person" nach § 203 StGB – mit eigener Strafbarkeit, wenn Mandanten- oder Patientendaten in ein Werkzeug gelangen, dessen Anbieter nicht seinerseits gebunden ist.

Rein KI-erzeugte Bilder und Texte haben keinen Urheberrechtsschutz (§ 2 Abs. 2 UrhG: nur persönliche geistige Schöpfungen). Wer einem Kunden ein „exklusives" KI-Logo verkauft, verkauft etwas, das jeder andere frei nutzen darf. Der Wiedererkennungswert einer Marke entsteht dann über Stil und Konsistenz, nicht über ein Ausschließlichkeitsrecht – das ist eine Eigenschaft, die man kennen sollte, kein Hindernis.

07

WAS EINE DATENSCHUTZERKLÄRUNG NICHT HEILT

Zwei Dinge, die ich unterschätzt hatte: **Das Verzeichnis der Verarbeitungstätigkeiten** (Art. 30 DSGVO) braucht praktisch jedes Unternehmen mit Kunden – die Ausnahme für Betriebe unter 250 Beschäftigten greift nur bei „gelegentlicher" Verarbeitung, und Kundendaten verarbeitet niemand gelegentlich. Jedes KI-Werkzeug gehört dort in die betroffenen Verarbeitungstätigkeiten: Zweck, Datenkategorien, Empfänger, Drittland, Löschfrist. Und **die Datenschutz-Folgenabschätzung** (Art. 35) ist bei einem Kunden-Chatbot, der die Interaktion mit Betroffenen steuert, in aller Regel Pflicht: Die deutsche Aufsicht führt den „Einsatz von künstlicher Intelligenz zur Steuerung der Interaktion mit den Betroffenen" auf ihrer Muss-Liste. Das interne Zusammenfassen einer Mail durch einen Mitarbeiter steht dort nicht – aber die Vorabprüfung, warum nicht, gehört in die Akte.

08

KENNTNIS MACHT ES BESSER, NICHT SCHLECHTER

Der Reflex, den ich selbst hatte, als der Befund auf dem Tisch lag: „Jetzt weiß ich es. Ab jetzt handle ich vorsätzlich – das ist schlimmer."

Das ist im Kern richtig beobachtet und in der Folge zu streng. Art. 83 Abs. 2 DSGVO nennt in lit. b tatsächlich Vorsätzlichkeit oder Fahrlässigkeit als Zumessungskriterium. Dieselbe Vorschrift bewertet aber in **lit. c** die Maßnahmen zur Minderung, in **lit. f** die Zusammenarbeit mit der Aufsicht und in **lit. h** die Art, wie der Verstoß bekannt wurde – insbesondere, ob man ihn selbst gemeldet hat.

Entscheidend ist nicht die Kenntnis, sondern was auf sie folgt. Wer einen Mangel selbst feststellt, ihn datiert festhält und abstellt, hat gute Gründe, besser dazustehen als jemand, der ihn nie bemerkt hat – eine Garantie ist das nicht. Schlechter steht nur, wer weiß und es dabei belässt.

Kenntnis macht es besser, nicht schlechter – solange auf sie etwas folgt.

Die praktische Folge, und sie ist der stärkste Gedanke dieses Textes: **Eine Aktenführung mit Datum, Messung und Beleg ist nicht nur Arbeitsmittel, sondern Nachweis der Bemühung.** Der Unterschied zwischen „wir haben ein Problem" und „wir haben ein Problem, hier ist seit wann wir es kennen, was wir gemessen haben und was wir getan haben" kann im Ernstfall einen erheblichen Unterschied machen.

09

DIE METHODE – SECHS REGELN, DIE ICH SEITHER ANWENDE

Was diesen Vorgang von einer Recherche unterscheidet, lässt sich als Verfahren beschreiben. Ich wende es inzwischen auf alles an, was ich für Kunden prüfe.

1. **Am Anbietertext des Tages messen, nie aus dem Gedächtnis.** Preise, Tarife und Vertragsbedingungen ändern sich. Eine Abschrift stimmt am Tag ihrer Entstehung – und danach nie wieder garantiert.
2. **Herkunft mitschreiben.** Zu jeder Zahl und jeder Aussage notieren, woher sie stammt: im Vertragstext gelesen, selbst gemessen, aus zwei anderen Werten abgeleitet, oder von jemandem mündlich gehört – und geschätzt gar nicht. Wer eine abgeleitete Zahl später als gemessen liest, baut auf Sand.
3. **Ein Ausschluss belegt nur den Ausschluss.** Aus „es gibt keine Rechnung“ folgt nicht „es gab keinen Vorgang“ – so bin ich in Abschnitt 5 bei den Nachkäufen gestolpert. Aus „der Anbieter sagt nichts zu X“ folgt nicht „X findet nicht statt“.
4. **Die Selbstbeschreibung eines Werkzeugs ist kein Beleg für seine Fähigkeiten.** Der KI-Kaufberater-Chat auf der Preisseite eines Anbieters hat mir in der Begrüßung versichert, er sehe meine Nutzungsdaten – und es im ersten Sachbeitrag zurückgenommen. Dasselbe gilt für Werbeseiten, Hilfetexte und Assistenten der Anbieter: Sie beschreiben ein Produkt, eine Vertragsgrundlage sind sie nicht.
5. **Anzeigen sind keine Messgrundlage.** Ein Bildschirm, der Prozentsätze einer nicht genannten und beweglichen Bezugsgröße zeigt, trägt keine Entscheidung (Abschnitt 5, der Verbrauchsbildschirm).
6. **Der eigene Fehler gehört in die Akte** – gekennzeichnet, datiert, nicht stillschweigend korrigiert.

10

SO BIN ICH VORGEGANGEN – ZEHN FRAGEN, DIE ICH MIR JE WERKZEUG GESTELLT HABE

Das ist kein Prüfschema für Ihren Betrieb, sondern die Reihenfolge, in der ich meinen geprüft habe. Sie hat sich bewährt, weil jede Frage die nächste kleiner macht.

1. **Was geht hinein?** Personendaten, Kundenmaterial, Quelltext, nichts davon? (Achse Inhalt)
2. **Wessen Daten sind es, und bin ich dafür verantwortlich?** (Achse Rolle)
3. **Welchen Tarif habe ich – Verbraucher oder kommerziell?** Nicht raten: Rechnung und Vertragstext ansehen. (Achse Produkt)
4. **Erlaubt der Tarif überhaupt geschäftliche Nutzung?** Nicht nur im Nutzungskapitel nachsehen – bei Anthropic stand der Satz im Haftungskapitel, bei Perplexity in der Lizenzklausel, bei Vercel in den Fair-Use-Richtlinien.
5. **Gibt es einen Auftragsverarbeitungsvertrag für genau diesen Tarif – und gilt er automatisch, per Klick oder erst nach Gegenzeichnung?**
6. **Ist Training vertraglich ausgeschlossen oder nur als Einstellung abgeschaltet?**
7. **Wer ist Vertragspartner, wo liegen die Daten, wo wird gerechnet?** Drei Antworten, nicht eine.
8. **Welche Fristen stehen im Vertrag** – Meldung bei Vorfall, Widerspruch bei Unterauftragnehmern – **und habe ich die Benachrichtigung abonniert?**
9. **Steht das Werkzeug in meinem Verarbeitungsverzeichnis und in meiner Datenschutzerklärung?**
10. **Was habe ich meinen Kunden vertraglich zugesagt – und hält der gewählte Tarif das?**

EIN NEIN BEI FRAGE 4 ODER 5 BEENDET DIE PRÜFUNG

Zehn Fragen je Werkzeug, in dieser Reihenfolge

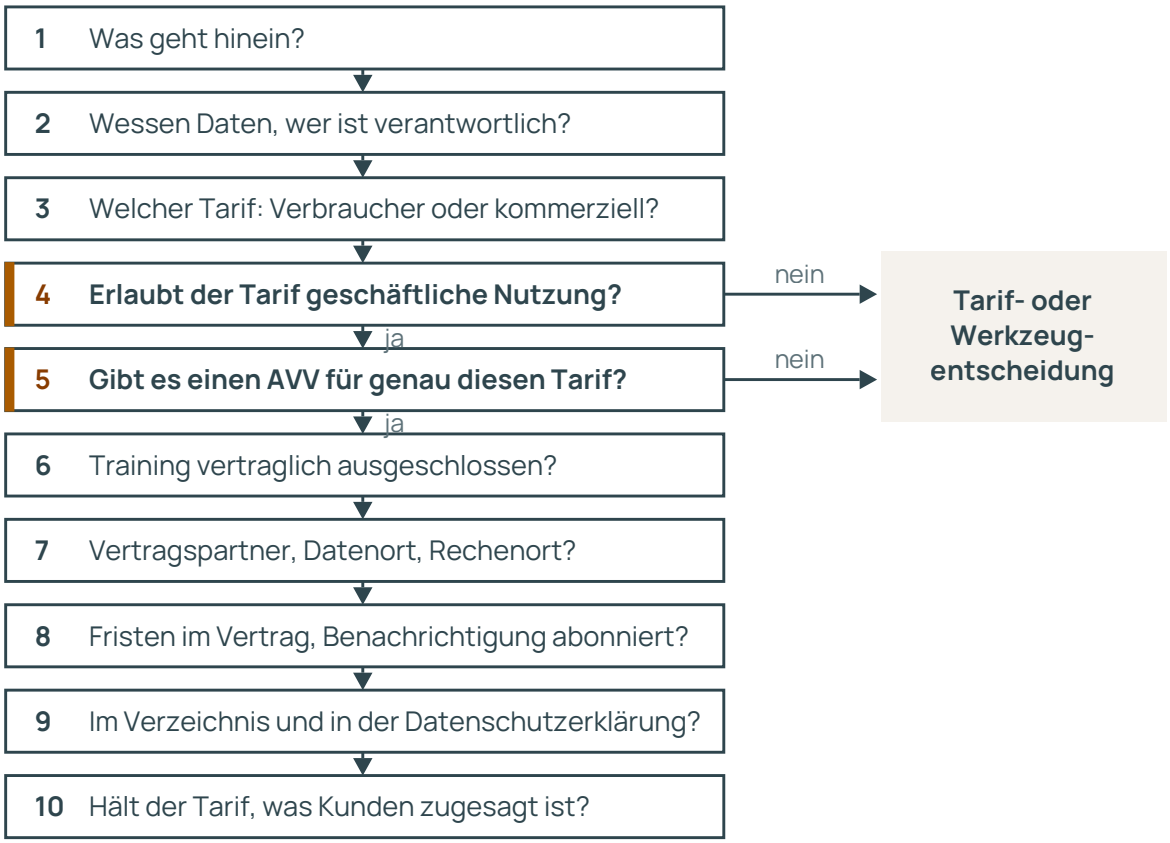

ABB. 5 · Nach einem Nein bei Frage 4 oder 5 entfallen die Fragen 6 bis 10: Dann ist zuerst über Tarif oder Werkzeug zu entscheiden. Eigene Darstellung

Wo ich bei Frage 4 oder 5 ein Nein bekam, brauchte ich die Fragen 6 bis 10 für dieses Werkzeug nicht mehr: Dann war es eine Tarif- oder Werkzeugentscheidung, keine Vertragsverhandlung.

WEITER IM GESPRÄCH

UND IHRE *Werkzeuge*?

Die zehn Fragen aus Teil B lassen sich allein abarbeiten. Wer dabei einen zweiten Blick möchte, kann mit mir darüber sprechen. Ich kenne die Stellen, an denen ich selbst hängen geblieben bin.

01

GESPRÄCH

Sie schildern, welche Werkzeuge Sie wofür einsetzen. Ich sage offen, ob und wo ich helfen kann.

02

BESTANDSAUFNAHME

Wir gehen Ihre Werkzeuge entlang der zehn Fragen durch, mit einem Befund je Werkzeug. Eine Rechtsberatung ersetzt das nicht.

03

UMSETZUNG

Aus dem Befund werden Entscheidungen: Tarif, Einstellungen, Verträge und eine Regel, die im Alltag hält.

KONTAKT

Andreas Riedel

Geschäftsführer · Wawayaro GmbH

E-MAIL info@wawayaro.com

TELEFON +49 30 60 93 56 53

WEB wawayaro.com/de#kontakt

Code antippen oder scannen: führt zum Kontakt auf wawayaro.com.

C

TEIL C

WERKZEUG-ANHANG, STAND 27.11.2026 (V2)

Lesehinweis. Dieser Anhang ist datiert und versioniert; er altert schneller als der Rest des Textes. Alle Angaben wurden am 27.11.2026 am Anbietertext gelesen, sofern nicht als sekundär (nur über Dritte belegt), nicht gemessen oder „nicht neu gemessen (Stand 03.09.2026)“ gekennzeichnet. Preise nenne ich nur, wo ich die Preisseite selbst gelesen habe; sie ändern sich häufiger als Vertragsklauseln.

„AVV automatisch“ heißt: Der Auftragsverarbeitungsvertrag wird durch Annahme der Nutzungsbedingungen Vertragsbestandteil. „AVV per Klick“: Er muss im Kundenportal ausgelöst werden – bis dahin gibt es ihn nicht. „AVV nach Gegenzeichnung“: Er wird erst mit Unterschrift des Anbieters wirksam.

C.1 KI-ASSISTENTEN IM CHAT

Zur Transparenz: Werkzeuge mit dem Kennzeichen „nutze ich“ setze ich derzeit selbst ein.

Werkzeug	Tarif	Geschäftsnutzung im Verbrauchertarif	AVV – ab welcher Stufe, Weg	Training (Standard)	Vertragspartner EWR · Region	Stolperstein	Quelle, Stand
Anthropic Claude	**Free / Pro / Max** Pro 17 USD/Monat jährlich bzw. 20 USD monatlich; Max ab 100 USD/Monat	**EWR-Fassung: verboten** – „Non-commercial use only“ (Abschn. 11). Zugang über Bot oder Skript nur mit API-Schlüssel (Abschn. 3). US-Fassung derselben URL: kein ausdrückliches Geschäftsverbot.	**Kein** AVV im Verbrauchertarif	Ja, sofern nicht in den Einstellungen abgeschaltet („unless you opt out … through your account settings“); Feedback bis 5 Jahre gespeichert	EWR-Fassung: Anthropic Ireland, Limited · US-Fassung: Anthropic, PBC · Inferenz: US	Dieselbe URL, zwei Verträge – je nach Standort des Lesers. Sperre ohne Ankündigung bei wesentlichem Verstoß, dann ohne Erstattung (EWR-Fassung Abschn. 13). Firmen-E-Mail-Domain kann das Konto an eine Organisation binden.	anthropic.com/legal/consumer-terms (wirksam 08.10.2025; EWR-Fassung aus einer EU-Umgebung, US-Fassung aus einer US-Umgebung abgerufen; Stand 27.11.2026); claude.com/pricing (Stand 27.11.2026); privacy.claude.com Artikel 10023580 (nicht neu gemessen, Stand 03.09.2026)
Anthropic Claude nutze ich	**Team** (Standard 20/25 USD, Premium 100/125 USD je Sitz und Monat, jährlich/monatlich; „teams of 2 to 150“) · **Enterprise** (nur Jahresabrechnung)	Vertragszweck (Commercial Terms: „not for consumer use“)	**Automatisch** – DPA „incorporated into these Terms by reference“ (Abschn. C)	**Vertraglich ausgeschlossen**: „Anthropic may not train models on Customer Content“ (Abschn. B)	Anthropic Ireland, Limited; irisches Recht · SCC Modul 2/3 im DPA · EU-Inferenz laut Regional-Compliance-Seite nur über AWS Bedrock/Google Vertex	Mindestens 2 Sitze. Subprozessor-Widerspruch 15 Tage (DPA C.3), Vorfallmeldung 48 h (G.1), Löschung 30 Tage (H.1). Zero Data Retention nicht im Standardplan. Beim Wechsel vom Verbraucherkonto wandern eigene Erweiterungen und Verbindungen nicht mit.	anthropic.com/legal/commercial-terms (17.06.2025); anthropic.com/legal/data-processing-addendum (24.02.2025); claude.com/pricing (alle Stand 27.11.2026);

Werkzeug	Tarif	Geschäftsnutzung im Verbrauchertarif	AVV – ab welcher Stufe, Weg	Training (Standard)	Vertragspartner EWR · Region	Stolperstein	Quelle, Stand
							claude.com/regional-compliance (nicht neu gemessen, Stand 03.09.2026)
OpenAI ChatGPT	**Free / Go / Plus / Pro** Preise nicht gemessen	Erlaubt, aber mit „Business use addendum“ in den EU-Terms (Haftung, Freistellung, kalifornisches Recht). Kein allgemeines Bot-Verbot, untersagt ist automatisiertes Auslesen. Plus/Pro dürfen ihr Kontingent laut OpenAI-Hilfe in freigegebenen Fremdwerkzeugen nutzen.	**Kein** AVV im Verbrauchertarif (Preisseite: Datenresidenz, SSO „No“)	Ja, Opt-out über Einstellungen/Privacy Portal; Temporary Chat nicht trainiert	OpenAI Ireland Ltd (EU-Terms) · Residenz: nein	Plus ist ein persönliches Abo; Auftragsverarbeitung erst ab Business. Sperre bei Verstoß, Vorankündigung nur angestrebt.	openai.com/policies/eu-terms-of-use (16.01.2026; Stand 27.11.2026); help.openai.com (Fremdwerkzeuge, Stand 27.11.2026); openai.com/policies/how-your-data-is-used-to-improve-model-performance (13.03.2026, nicht neu gemessen); chatgpt.com/pricing (Beträge nicht lesbar)
OpenAI ChatGPT	**Business / Enterprise** ab 2 Nutzern; Preis nicht gemessen	Vertragszweck	**Automatisch** – „DPA … incorporated by this reference“ (Services Agreement 5.3); zusätzlich gesonderte Unterzeichnung möglich	**Vertraglich ausgeschlossen** („will not use Customer Content to develop or improve“, 4.2)	OpenAI Ireland Ltd · Datenresidenz US/EU/UK u. a. laut Preisseite; Zuordnung Business/Enterprise nicht eindeutig gemessen	Subprozessor-Widerspruch 30 Tage (DPA 2.9); Vorfallmeldung nur „without undue delay“; Schiedsverfahren in San Francisco trotz irischem Recht	openai.com/policies/services-agreement (01.01.2026); openai.com/policies/data-processing-addendum (01.01.2026) (beide Stand 27.11.2026)
Google Gemini-App	**Verbraucherkonto**	nicht gemessen (Google-Nutzungsbedingungen nicht ausgewertet)	**Kein** AVV für Privatkonten	Ja bei eingeschaltetem „Gemini-Verlauf“; **menschliche Prüfer lesen eine Teilmenge**; geprüfte Chats bis 3 Jahre – auch nach Löschung	Google Ireland Limited	Googles eigene Warnung: keine vertraulichen Informationen eingeben. Auto-Löschung Standard 18 Monate.	support.google.com/gemini/answer/13594961 (Stand 24.11.2026)

Werkzeug	Tarif	Geschäftsnutzung im Verbrauchertarif	AVV – ab welcher Stufe, Weg	Training (Standard)	Vertragspartner EWR · Region	Stolperstein	Quelle, Stand
Google Gemini	**in Google Workspace**	Geschäftsprodukt	Cloud Data Processing Addendum, Bestandteil der Workspace-Bedingungen (automatisch)	Vertragliche Zusage: keine Nutzung zum Training außerhalb der Organisation	Google Ireland Ltd · Datenregion je Edition (nicht gemessen)	Unterschied zum Gratiskonto ist rein vertraglich, nicht technisch	workspace.google.com/security/ai-privacy (Stand 27.11.2026); knowledge.workspace.google.com (Privacy Hub, nicht neu gemessen)
Microsoft Copilot	**Verbraucher**	**Nur private Nutzung** („for your own personal use"); Bots und Scraper untersagt	**Kein** DPA (Verbrauchervertrag)	Inhalte zum Betreiben und Verbessern; Steuerung über Datenschutzoptionen, ausdrückliche Trainingsklausel nicht im Text	Microsoft (EU-Gesellschaft im Text nicht genannt)	„Copilot" heißt Verbraucher- und Geschäftsprodukt gleichermaßen; mit Arbeitskonto gelten andere Bedingungen	microsoft.com/microsoft-copilot/for-individuals/termsofuse (wirksam 18.08.2026; Stand 27.11.2026)
Microsoft 365 Copilot	**Geschäftskunden**	Geschäftsprodukt	**Automatisch** – Microsoft Products and Services DPA über die Product Terms	Vertraglich: Prompts, Antworten, Graph-Daten „aren't used to train foundation LLMs"	Microsoft Ireland Operations Ltd (nicht gemessen) · EU Data Boundary – **Ausnahme: Anthropic-Modelle als Subprozessor**	Bei hoher Auslastung können Anfragen in andere Regionen laufen; für EU-Verkehr gilt laut Seite die EU Data Boundary. „Flex Routing" standardmäßig aktiv: nur sekundär belegt	learn.microsoft.com Copilot Privacy (Stand 03.11.2026); Message Center MC1269223 (sekundär, nicht neu gemessen)
Mistral Le Chat	**Free / Pro**	**Nur private Nutzung** („in your personal capacity"); Geschäftskunden auf die Commercial Terms verwiesen	**Kein** AVV für Verbraucher	Ja, außer Opt-out; Feedback erlaubt Training samt Ein- und Ausgabe	Mistral AI SAS, Paris	–	legal.mistral.ai/terms/eu-consumers-terms-of-service (wirksam 08.10.2026; Stand 27.11.2026)
Mistral Le Chat	**Team / Enterprise · La Plateforme (API)**	Geschäftsprodukt	DPA gilt, wenn Mistral als Auftragsverarbeiter tätig ist (Commercial Terms 12.3; DPA 1 (a), 11.2)	**Eingeschränkt**: Mistral darf laut DPA 2.3 als Verantwortlicher trainieren, „unless Customer … has op-	Mistral AI SAS, Paris – EU-Sitz, kein Drittlandtransfer durch den Anbieter selbst		legal.mistral.ai/terms/data-processing-addendum (27.07.2026); …/com-

Werkzeug	Tarif	Geschäftsnutzung im Verbrauchertarif	AVV – ab welcher Stufe, Weg	Training (Standard)	Vertragspartner EWR · Region	Stolperstein	Quelle, Stand
				ted-out"; Labs/Preview-Modelle trainieren immer (Commercial Terms 4.3)		Der EU-Sitz ersetzt die Prüfung der Trainingsklausel nicht. Subprozessor-Widerspruch 10 Tage; Vorfallmeldung „without undue delay"	mercial-terms-of-service (wirksam 25.09.2026) (beide Stand 27.11.2026)
Perplexity	**Free / Pro**	Fassung vom 23.01.2026: „personal, non-commercial use only" (5.1). Neue Fassung, wirksam 01.01.2027: persönliche Lizenz, ausdrückliches Geschäftsverbot entfällt	**Kein** AVV; Enterprise-Terms gesondert (nicht gemessen)	Lizenz zur Nutzung der Inhalte „to operate, improve … the Services" (6.4(b)); Opt-out nicht gemessen	Perplexity AI, Inc., USA – keine EU-Gesellschaft gefunden; Schiedsklausel mit 30 Tagen Opt-out	Bedingungen wechseln zum 01.01.2027; ob bis dahin die alte Fassung gilt, ist nicht gemessen – Fassung des Tages prüfen	perplexity.ai/hub/legal/terms-of-service (Fassung wirksam 01.01.2027; Stand 27.11.2026)
DeepSeek	**App/Web**	nicht gemessen	**Kein** AVV gefunden	Ja („to train and improve … machine learning models"), Opt-out nur per E-Mail-Anfrage	Hangzhou DeepSeek, China – Speicherung „in People's Republic of China"	Italienische Aufsicht sperrte 2025 die Verarbeitung; Berliner Aufsicht meldete die App 2025 an die App-Stores	cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html (10.02.2026; Stand 27.11.2026); netzpolitik.org 2025; euronews 31.01.2025
xAI Grok	**Verbraucher**	Enterprise-Terms für Unternehmen vorgesehen; Verbot im Verbrauchertext nicht gemessen	**Kein** DPA im Verbrauchervertrag	Opt-out als Einstellung	nicht gemessen	Konten mit Firmen-Domain können an ein Enterprise-Abo gebunden werden	x.ai/legal/terms-of-service (01.09.2026) · nicht neu gemessen (Stand 03.09.2026; Seite am 27.11.2026 nicht abrufbar, laut Suche inzwischen neuere Fassungen)

C.2 PROGRAMMIERSCHNITTSTELLEN UND CODING-WERKZEUGE

Zur Transparenz: Werkzeuge mit dem Kennzeichen „nutze ich“ setze ich derzeit selbst ein.

Werkzeug	Tarif	Geschäftsnutzung	AVV	Training (Standard)	Vertragspartner · Region	Stolperstein	Quelle, Stand
Anthropic API / Console nutze ich	nutzungsabhängig	Vertragszweck (Commercial Terms ab erstem Schlüssel)	**Automatisch** (Abschn. C)	**Vertraglich ausgeschlossen** (Abschn. B)	Anthropic Ireland · Inferenz US; EU nur über Bedrock/Vertex	Standard-Aufbewahrung 30 Tage; Zero Data Retention nur per Vereinbarung	anthropic.com/legal/commercial-terms (Stand 27.11.2026); privacy.claude.com Artikel 7996866 (01.07.2026, nicht neu gemessen)
Claude Code	**Anmeldung über Verbraucherabo (Pro/Max)**	siehe C.1 Verbraucher	**Kein** AVV	Training möglich, wenn Einstellung an; Aufbewahrung 5 Jahre (an) / 30 Tage (aus)	wie C.1	**Dieselbe Software, anderer Vertrag – die Anmeldeart entscheidet.** Abo-Login laut Anthropic nur für die übliche Nutzung in Anthropics eigenen Anwendungen; Fremdwerkzeuge und Agent SDK über API-Schlüssel, Durchsetzung ohne Vorankündigung	code.claude.com/docs/en/data-usage; code.claude.com/docs/en/legal-and-compliance (beide ohne Datum; Stand 27.11.2026)
Claude Code nutze ich	**über API-Schlüssel / Team / Enterprise**	Vertragszweck	Automatisch	Vertraglich ausgeschlossen	Anthropic Ireland	ZDR „not included in the standard Enterprise plan“	ebd. (Stand 27.11.2026)

Werkzeug	Tarif	Geschäftsnutzung	AVV	Training (Standard)	Vertragspartner · Region	Stolperstein	Quelle, Stand
OpenAI API nutze ich (Bilderzeugung)	nutzungsabhängig; EU-Residenz mit 10 % Aufschlag	Geschäftsangebot	**Gesondert** – DPA-Formular (Ironclad) ausfüllen	**Kein Training seit 01.03.2023**	Vertragspartner nicht gemessen · EU-Residenz eu.api.openai.com nur nach Freigabe durch Sales plus „Modified Retention amendment“	Abuse-Monitoring-Logs 30 Tage Standard; ZDR nur auf Antrag	openai.com/enterprise-privacy (08.01.2026); developers.openai.com/api/docs/guides/your-data · nicht neu gemessen (Stand 03.09.2026)
Google AI Studio / Gemini API, unbezahlte Stufe	–	Nur für „professional or business purposes“ – aber **Endkunden im EWR nur über Paid Services**	Außerhalb EWR: kein Processor-DPA. **EWR/CH/UK: seit 23.03.2026 gelten die Paid-Regeln auch für die Gratisstufe**	**Außerhalb EWR: Training plus menschliche Durchsicht**; Vertragstext selbst: „Do not submit sensitive, confidential, or personal information to the Unpaid Services“	Google-Entity je Cloud-Terms · keine Regionsgarantie	Ein Prototyp auf Gratis-Quota, der EU-Endkunden erreicht, ist laut Use Restrictions nicht erlaubt	ai.google.dev/gemini-api/terms (wirksam 23.03.2026, Seitenstand 28.04.2026; abgerufen 27.11.2026)
Google Gemini API	**bezahlt / Vertex AI**	Geschäftsangebot	**Automatisch** (Processor-DPA per Verweis)	Kein Training	EU-Inferenz nur über Vertex mit EU-Region (nicht gemessen)	Grounding-Daten 30 Tage gespeichert	ebd. (Stand 27.11.2026; Speicherdauer der Grounding-Daten nicht neu gemessen)
Microsoft Azure OpenAI / Foundry	–	B2B	**Automatisch** (aka.ms/DPA)	Kein Training	Deployment-Typ entscheidet: „Standard“ und „DataZone EU“ bleiben in der EU, **„Global“ nicht**	Missbrauchsüberwachung ist Standard, menschliche Prüfung bei markierten Inhalten. Die Abschaltung auf Antrag wird für Modelle ab 01.11.2026 eingestellt	learn.microsoft.com Azure Foundry data-privacy (Stand 05.06.2026, Änderungen bis 17.11.2026)

Werkzeug	Tarif	Geschäftsnutzung	AVV	Training (Standard)	Vertragspartner · Region	Stolperstein	Quelle, Stand
AWS Bedrock	–	B2B	Automatisch (AWS DPA in den Service Terms; Dokument nicht gemessen)	Kein Training durch Modellanbieter	EU-Regionen wählbar	**ZDR gilt nicht für jedes Modell**: für Claude Fable 5, 5.1 und 5.2 wird der gesamte Verkehr bis 30 Tage gespeichert, markierter Verkehr ggf. menschlich geprüft	docs.aws.amazon.com/bedrock abuse-detection (ohne Datum; Stand 27.11.2026); data-protection (nicht neu gemessen)
GitHub Copilot	**Free / Pro / Pro+**	nicht gemessen	**Kein** DPA für Einzelpläne	**Seit 24.04.2026 Training mit Interaktionen, Opt-out nötig**	nicht gemessen	Der Opt-out-Schalter steht nur in den persönlichen Einstellungen des Nutzers	docs.github.com/copilot/how-tos/manage-your-account/manage-policies (Stand 27.11.2026)
GitHub Copilot	**Business / Enterprise**	Organisationslizenz	**Automatisch** (GitHub DPA)	Kein Training	nicht gemessen	Trainingsschalter wird gar nicht angezeigt	ebd. (Stand 27.11.2026)
Cursor	**Hobby / Pro / Teams** Preise sekundär	nicht gemessen	nicht gemessen	**Abhängig vom Privacy Mode** – ohne ihn darf Cursor Codebasis, Prompts und Editor-Aktionen zum Training nutzen	Anysphere, Inc., USA	Auch mit eigenem API-Schlüssel laufen alle Anfragen über Cursors Backend	cursor.com/data-use (Seitenstand 03.09.2026; abgerufen 27.11.2026)

C.3 BILD- UND MEDIENGENERATOREN

Zur Transparenz: Werkzeuge mit dem Kennzeichen „nutze ich“ setze ich derzeit selbst ein.

Werkzeug	Tarif	Geschäftsnutzung	AVV	Training / Lizenz an den Anbieter	Vertragspartner	Stolperstein	Quelle, Stand
OpenAI Bilderzeugung nutze ich (per API)	**in ChatGPT / per API**	Erlaubt; Output-Rechte „if any“ zugewiesen	ChatGPT: kein AVV (Verbraucher) · API: DPA gesondert	ChatGPT: Training Standard, Opt-out · API: kein Training	OpenAI Ireland (EU-Terms)	„Output may not be unique“ – gleicher Output bei anderen Nutzern möglich; Verbot, Output als menschengemacht darzustellen	openai.com/policies/row-terms-of-use (01.01.2026; Stand 27.11.2026)
Midjourney	**Basic / Standard / Pro / Mega** 10 / 30 / 60 / 120 USD/ Monat	Ja – **aber**: Unternehmen (und „any employee of a company“) mit mehr als 1 Mio. USD Jahresumsatz nur mit Pro/Mega Eigentum an den Bildern	**Kein** DPA gefunden	**Ewige, unwiderrufliche Lizenz an Midjourney** an Eingaben und Bildern, überlebt die Kündigung; Trainingsklausel in Privacy Policy (sekundär)	Midjourney, Inc., USA; kalifornisches Recht	Ohne Stealth Mode (nur Pro/Mega) sind alle Bilder öffentlich und remixbar – auch unveröffentlichte Kundenentwürfe	docs.midjourney.com Terms of Service (27.05.2026; Stand 27.11.2026); Plan-Vergleich (nicht neu gemessen, Seite nicht abrufbar)
Adobe Firefly	–	Ja („commercially safe“)	Adobe-DPA für Geschäftskunden (nicht gemessen)	Training auf lizenzierten Inhalten und gemeinfreien Werken (Anbieteraussage)	Adobe Systems Software Ireland (nicht gemessen)	IP-Freistellung nur für „qualifying plans“; Content Credentials automatisch bei vollständig erzeugten Inhalten (Art. 50 Abs. 2)	business.adobe.com Firefly AI approach (18.03.2025; Stand 27.11.2026)
Canva Magic Studio	**Free / Pro**	Ja	**Kein** DPA für Free/Pro (sekundär); DPA für Teams/Enterprise	**Training standardmäßig an**, Opt-out in den Datenschutz-Einstellungen (sekundär)	Canva Pty Ltd, Australien	Freistellung nur „eligible enterprise customers“	canva.com/safe-ai-canva-shield; compound.law (sekundär) · nicht neu gemessen (Stand 03.09.2026; Seiten am 27.11.2026 nicht abrufbar)

Werkzeug	Tarif	Geschäftsnutzung	AVV	Training / Lizenz an den Anbieter	Vertragspartner	Stolperstein	Quelle, Stand
Stability AI Stable Diffusion	**Community License, Selbsthosting**	Frei unter 1 Mio. USD Jahresumsatz – darüber Enterprise-Lizenz nötig	Nicht einschlägig – Selbsthosting	Kein Training durch Anbieter möglich	Selbst gewählt	Wer selbst hostet, wird **Anbieter** nach der KI-Verordnung – mit Markierungspflicht nach Art. 50 Abs. 2	stability.ai/license (Stand 27.11.2026)
Ideogram	**Free / bezahlt / Self-Serve License** 300 USD/Monat Selbsthosting	Ja	nicht gemessen	nicht gemessen (auf der Lizenzseite nicht beschrieben)	Ideogram, Inc., USA	Forschungslizenz der offenen Gewichte erlaubt keine kommerzielle Nutzung	ideogram.ai/licensing (Stand 27.11.2026)

Rechtlicher Rahmen für alle Bildwerkzeuge (Stand 27.11.2026): Kennzeichnungspflicht Art. 50 KI-VO gilt seit 02.08.2026; für Systeme, die vor diesem Tag in Verkehr waren, gilt die maschinenlesbare Markierung nach Abs. 2 mit Übergangsfrist bis 02.12.2026. Die maschinenlesbare Markierung (Abs. 2) trifft den Anbieter; die sichtbare Offenlegung eines Deepfakes (Abs. 4) trifft den Betreiber – **und die Markierung des Anbieters genügt dafür nicht** (EU-Kommission, FAQ Art. 50, Stand 24.07.2026). Ein KI-Symbolbild eines erfundenen Büros ist kein Deepfake; das fotorealistische KI-Bild des Geschäftsführers auf einer Messe, auf der er nie war, ist einer, wenn es als echtes Foto erscheint. Rein KI-erzeugte Bilder haben keinen Urheberrechtsschutz (§ 2 Abs. 2 UrhG; in den USA: der Supreme Court hat die Revision in Thaler v. Perlmutter am 02.03.2026 nicht angenommen, es bleibt bei der Entscheidung des Berufungsgerichts). Was ich selbst mache, ohne dass es Pflicht wäre: ein Satz im Bildnachweis – „Illustrationen KI-erzeugt (Anbieter)“. Kostet keine Wirkung, erledigt jeden Grenzfall mit.

C.4 GESPRÄCHSAUFZEICHNUNG, TRANSKRIPTION, MEETING-ASSISTENTEN

Zur Transparenz: Werkzeuge mit dem Kennzeichen „nutze ich“ setze ich derzeit selbst ein.

Werkzeug	Tarif	Verlässt Audio das Gerät?	AVV	Training	Verarbeitungsort · Vertragspartner	Stolperstein	Quelle, Stand
MacWhisper nutze ich	Good Snooze, NL; Einmalkauf	**Nein** bei lokaler Transkription – **ja**, wenn ein Cloud-Anbieter (z. B. Groq, ElevenLabs, Deepgram) aktiviert wird; auch DeepL-Übersetzung und KI-Prompts senden Text hinaus	Lokal nicht nötig; bei Cloud-Anbieter dessen AVV	Lokal: kein Training möglich	Gerät	„Lokal“ ist eine Einstellung, kein Produktversprechen	docs.macwhisper.com Artikel 52 (Stand 27.11.2026)
Apple Sprachmemos / Notizen / Telefonaufnahme mit Transkription nutze ich	–	Transkription lokal (Neural Engine) laut Fachquellen; Apple-Primärquelle nicht gemessen · Zusammenfassung kann an Private Cloud Compute gehen	Kein AVV (Verbraucher, siehe C.6)	Kein Training angegeben (nicht gemessen)	Gerät · Apple	iOS kündigt bei Telefonaufnahme allen Teilnehmern die Aufnahme akustisch an	appleinsider 04.09.2024; get-inscribe.com (beide sekundär) · nicht neu gemessen (Stand 03.09.2026)
whisper.cpp	Open Source	Nein	Nicht nötig	Nein	Gerät	Kommandozeile – Hürde für Nichttechniker	github.com/ggml-org/whisper.cpp (Stand 27.11.2026)
Otter.ai	**Free / Pro**	Ja	**Kein** DPA für Free/Pro	Training mit de-identifizierten Daten (die Stimme ist gleichwohl biometrisch); ob Standard und wie Opt-out, beschreibt die Anbieterseite nicht	Otter.ai Inc., USA; AWS S3, Region nicht angegeben	US-Sammelklage 2025 wegen Trainingsnutzung (sekundär)	otter.ai/privacy-security (Stand 27.11.2026); DPA-Angabe und Sammelklage nicht neu gemessen

Werkzeug	Tarif	Verlässt Audio das Gerät?	AVV	Training	Verarbeitungsort · Vertragspartner	Stolperstein	Quelle, Stand
Fireflies.ai	–	Ja (Bot tritt dem Meeting bei)	Auf der Sicherheitsseite kein DPA genannt (BAA/DSA nur Enterprise)	Kein Training mit Meetingdaten	Standardort nicht genannt; Enterprise: Speicherung am gewählten Ort	„GDPR compliant" auf der Website ist kein EWR-Verarbeitungsort	fireflies.ai/security (Stand 27.11.2026)
tl;dv	**Free / Pro / Business**	Ja	Kein DPA genannt; Standardvertragsklauseln und Weisungsbindung laut Datenschutzerklärung	Kein Training eigener Modelle mit Kundeninhalten	Tldx Solutions GmbH, Aachen; Verarbeitung überwiegend im EWR, KI-Hosting EU oder USA wählbar	Bei KI-Hosting USA gehen Transkriptteile in die USA	tldv.io/privacy (Stand 27.11.2026)
Zoom	**AI Companion** in bezahlten Plänen	Ja	Zoom Global DPA Teil der Nutzungsbedingungen	Ausschluss laut Anbieterseite (sekundär); vertragliche Verankerung nicht gemessen	Zoom, USA; EU-Rechenzentren wählbar (nicht gemessen)	2023 stand eine Trainingsklausel wochenlang in den Terms – Klauseln ändern sich per Update	zoom.com AI Companion privacy (sekundär); media.zoom.com Global DPA · nicht neu gemessen (Stand 03.09.2026; Seite am 27.11.2026 nicht lesbar)
Microsoft Teams Copilot / Intelligent Recap	–	Ja	Microsoft DPA automatisch	Kein Training	EU Data Boundary, aber Flex Routing (siehe C.1)	Transkripte: 60 Tage Standard plus 93 Tage Papierkorb – Löschzusagen an Kunden müssen dazu passen (sekundär)	learn.microsoft.com (sekundär) · nicht neu gemessen (Stand 03.09.2026)
Google Meet „Notizen mit Gemini"	–	Ja	Workspace CDPA automatisch	Kein Training außerhalb der Organisation	Google Cloud EMEA (nicht gemessen)	Notizen landen als Google Doc im Drive des Organisators	blog.google; knowledge.workspace.google.com (sekundär) · nicht neu gemessen (Stand 03.09.2026)

Werkzeug	Tarif	Verlässt Audio das Gerät?	AVV	Training	Verarbeitungsort · Vertragspartner	Stolperstein	Quelle, Stand
Plaud Note / NotePin	Hardware plus Cloud-Abo	Ja (Cloud-Transkription)	Seite „Data Processing Addendum“ vorhanden (Inhalt nicht gemessen)	Kein Training ohne vorherige ausdrückliche Einwilligung	Plaud Inc., Delaware, als Verantwortlicher; Server in USA, Deutschland, Japan, Singapur, **Speicherung in der Region des Nutzers**	**Bewusst unauffälliges Gerät: wer es im Kundengespräch laufen lässt, ohne es anzusagen, riskiert § 201 StGB**	eu.plaud.ai/policies/privacy-policy (gültig ab 21.11.2026; Stand 27.11.2026)
Notion	**AI Meeting Notes**	Ja, Echtzeit an Subprozessoren	Notion DPA „available for all customers“	Vertraglicher Ausschluss bei Subprozessoren	Notion Labs, USA	Im Fehlerfall Audio bis 3 Tage (Desktop/Browser) bzw. bis 30 Tage (mobil) bei Notion; LLM-Aufbewahrung 30 Tage außer Enterprise (nicht neu gemessen)	notion.com/help/ai-meeting-notes-security-and-privacy (Stand 27.11.2026); notion.com/help/notion-ai-security-practices und DPA-Angabe (nicht neu gemessen)

Rechtlicher Rahmen (alle Werkzeuge dieser Kategorie): § 201 StGB – Einwilligung **aller** Sprechenden **vor** dem Start der Aufnahme; der Aufnahmehinweis der Plattform informiert, er holt keine Einwilligung ein und belegt nicht, wer zugestimmt hat. Bei Coaching, HR- und Gesundheitsthemen: Art. 9 DSGVO, ausdrückliche Einwilligung. Die Stimme selbst ist ein biometrisches Merkmal, sobald sie zur Sprechererkennung genutzt wird. Ein Bot, der nur mithört und zusammenfasst, löst Art. 50 Abs. 1 KI-VO eher nicht aus; ein KI-System, das im Gespräch antwortet oder Interviews führt, schon (Anbieterpflicht). Was ich selbst mache: Aufnahme und Transkription laufen lokal; aus dem Transkript entferne ich von Hand, was eventuell zu Gesundheit, Familie und Privatleben angefallen ist – die Namen bleiben, sonst wüsste ich hinterher nicht mehr, mit wem ich gesprochen habe; erst dann in ein Werkzeug mit Geschäftsvertrag. Dazu ein Hinweisblatt für Gesprächspartner, das genau dieses Verfahren beschreibt (bei mir in Arbeit).

Wichtig: Wer ein Verfahren beschreibt, muss es auch einhalten.

C.5 HOSTING, DATENBANK, VERSAND, ANALYSE, CODE-HOSTING

Zur Transparenz: Werkzeuge mit dem Kennzeichen „nutze ich“ setze ich derzeit selbst ein.

Werkzeug	Tarif	Geschäftsnutzung im Gratistarif	AVV – Stufe und Weg	Vertragspartner · Region	Drittlandgrundlage	Stolperstein	Quelle, Stand
Vercel	**Hobby** 0 USD	**Verboten**: nur „personal or non-commercial use“ (Terms, Abschn. 4)	DPA gilt **nur für Pro und Enterprise** (DPA Introduction)	Vercel Inc., USA; „primary processing facilities are in the United States“	SCC; DPF nicht genannt	Runtime-Logs 1 Stunde (Hobby), 1 Tag (Pro), 30 Tage mit Observability Plus (vercel.com/docs/logs/runtime, nicht neu gemessen) – eine Datenschutzerklärung, die „7 Tage“ nennt, stimmt damit nicht überein; meine tat es. Widerspruch gegen neue Unterauftragnehmer 5 Tage, Mitteilung nur nach E-Mail-Anmeldung	vercel.com/legal/terms (19.10.2026); vercel.com/legal/dpa (17.03.2026); vercel.com/docs/plans/hobby (12.11.2026) (alle Stand 27.11.2026)
Vercel	**Pro** Preis nicht gemessen	Vertragszweck	Automatisch	wie oben	wie oben	Löst mit einem Zug drei Befunde (Nutzung, AVV, Logs)	ebd. (Stand 27.11.2026)
Netlify	**Free / Pro**	nicht gemessen (Subscription Agreement nur als PDF)	DPA existiert; ob Free abgedeckt ist: **widersprüchliche Angaben, nicht gemessen**	Netlify, Inc., USA	nicht gemessen	–	netlify.com/legal/terms-of-use (14.10.2026; Stand 27.11.2026); DPA-Abdeckung Free nicht neu gemessen

Werkzeug	Tarif	Geschäftsnutzung im Gratistarif	AVV – Stufe und Weg	Vertragspartner · Region	Drittlandgrundlage	Stolperstein	Quelle, Stand
netcup nutze ich	Karlsruhe	Geschäftskunde regulär	**Per Klick** im Kundencenter (CCP): Stammdaten › Auftragsverarbeitung › „AV-Vertrag erstellen"; elektronische Unterschrift genügt	netcup GmbH, DE; Rechenzentren Nürnberg/Wien (Anbieterangabe)	Kein Drittland	Ohne Klick kein Vertrag – obwohl der Server in Deutschland steht	netcup Helpcenter „DPA" (Stand 20.11.2026)
Hetzner	Gunzenhausen	Geschäftskunde regulär	**Per Klick**: accounts.hetzner.com/account/dpa; Hetzner unterschreibt keine individuellen AVV	Hetzner Online GmbH, DE; EU: Falkenstein, Nürnberg, Helsinki; Cloud zusätzlich USA und Singapur wählbar	Kein Drittland bei EU-Standort; Cloud-Region wird beim Anlegen gewählt	Region wird beim Anlegen gewählt; Kunden-Stammdaten bleiben in der EU	docs.hetzner.com Datenschutz-FAQ (Stand 27.11.2026)
IONOS	Montabaur	Ja	**Per Klick** im Kundenkonto (sekundär)	IONOS SE, DE	Kein Drittland	–	gehrke-media.de (sekundär) · nicht neu gemessen (Stand 03.09.2026; Anbieterseite am 27.11.2026 nicht abrufbar)
Strato nutze ich	Berlin; Hosting und E-Mail	Ja	AVV Version 3.5 ist Teil der AGB der gebuchten Produkte (Ziff. 12.3); Altverträge: Weg im Kundenlogin prüfen	STRATO GmbH, DE	Kein Drittland	Ob ältere Verträge ohne eigenen Klick erfasst sind, sagt die AVV-Seite nicht – Stichtag prüfen	strato.de/agb/avv (V 3.5, 18.03.2024; Stand 27.11.2026)
Railway	–	nicht gemessen	**Nach Gegenzeichnung** (DocuSign) – „binding upon Company's execution"	Railway Corp., USA; lokale Speicherorte nur für zahlende Kunden	DPF oder SCC	Widerspruch 10 Tage, Abonnement der Benachrichtigung ausdrücklich verlangt	railway.com/legal/dpa (Stand 27.11.2026)

Werkzeug	Tarif	Geschäftsnutzung im Gratistarif	AVV – Stufe und Weg	Vertragspartner · Region	Drittlandgrundlage	Stolperstein	Quelle, Stand
Cloudflare nutze ich	**Free / Pro / Business** DNS, Reverse Proxy, Turnstile	Ja	**Automatisch für alle Self-Serve-Kunden inkl. Free** – DPA „incorporated by reference“ ins Self-Serve Subscription Agreement	Cloudflare, Inc., USA; Verarbeitungsort ohne Enterprise-Add-on nicht steuerbar	**DPF-zertifiziert** plus SCC	Jeder Aufruf jeder Seite läuft samt IP-Adresse durch Cloudflare – gehört in Datenschutzerklärung und Verzeichnis. Subprozessor-Widerspruch 10 Tage, keine aktive Benachrichtigung	cloudflare.com/cloudflare-customer-dpa (v6.4, 03.04.2026; Stand 27.11.2026); cloudflare.com/terms
Supabase nutze ich	**Free / Pro**	Ja	**Automatisch für alle Pläne** – „supplements and forms part of the … Terms of Service“; „acceptance … shall have the same effect as signing the SCCs“ (12.2)	**Supabase Pte. Ltd, Singapur** (Drittland ohne Angemessenheitsbeschluss) · Region beim Anlegen wählbar, Frankfurt verfügbar	SCC Modul 2/3, irisches Recht	Region ist eine Entscheidung, keine Voreinstellung (6.1). 30 Tage Vorlauf nur für Abonnenten der Subprozessor-Liste, **Widerspruch 5 Tage** (6.3). Vorfallmeldung „where feasible“ 48 h	supabase.com/legal/customer-resources/data-processing-addendum (Version 1, 01.08.2026; Stand 27.11.2026)
Neon	–	nicht gemessen	Automatisch („embedded in our terms“, Blog)	Neon Inc., USA; Frankfurt wählbar	nicht gemessen	–	neon.tech/dpa (Stand 27.11.2026); neon.com/blog/gdpr-compliance-and-neon (12.02.2025); Frankfurt-Region nicht neu gemessen
MongoDB Atlas	–	nicht gemessen	Automatisch (Teil der Cloud Terms)	MongoDB, Inc. als SCC-Importeur; EU-Gesellschaft nicht genannt	SCC	Free-Tier nur in wenigen Regionen; Subprozessor-Mitteilung 30 Tage vorher nur nach Anmeldung, Widerspruch ohne feste Frist	mongodb.com/legal/data-processing-agreement (21.10.2024; Stand 27.11.2026)

Werkzeug	Tarif	Geschäftsnutzung im Gratistarif	AVV – Stufe und Weg	Vertragspartner · Region	Drittlandgrundlage	Stolperstein	Quelle, Stand
Airtable	–	nicht gemessen	**Nach Gegenzeichnung** (Formular › DocuSign); laut Anbieter „All plan types“	Airtable, Inc., USA	nicht gemessen	EU-Datenresidenz nur für Base-Inhalte in höheren Tarifen (sekundär)	support.airtable.com Artikel 4245698629 · nicht neu gemessen (Stand 03.09.2026; Seite am 27.11.2026 nicht abrufbar)
AWS / Azure / Google Cloud	–	Ja	Automatisch (DPA in den Terms)	EU-Gesellschaften (nicht gemessen) · EU-Regionen wählbar	SCC; DPF (nicht gemessen)	Region muss je Ressource aktiv gewählt werden	cloud.google.com/terms/data-processing-addendum (Stand 27.11.2026); aws.amazon.com/service-terms; aka.ms/DPA (beide nicht neu gemessen, Stand 03.09.2026)
Resend nutze ich	Transaktions-E-Mail	nicht gemessen	**Automatisch** – „legally binding upon Customer entering into the Agreement“; unterschriebene Fassung im Dashboard	Plus Five Five, Inc., USA; „primary processing operations … in the United States“	**DPF-zertifiziert** plus SCC	Widerspruch 14 Tage. Open-/Click-Tracking erfasst laut Exhibit A IP, Standort, Gerät – eine eigene Verarbeitung, die eine Rechtsgrundlage braucht	resend.com/legal/dpa (Seitenangabe „Last updated“ 31.12.2025; Stand 27.11.2026)
Postmark	–	kein Free-Tarif	Automatisch	AC PM LLC (ActiveCampaign), USA	DPF plus SCC	Benachrichtigung nur nach Formular-Anmeldung, **Widerspruch 7 Tage**	postmarkapp.com/dpa (wirksam 17.11.2025; Stand 27.11.2026)
Brevo	Paris	nicht gemessen	Automatisch (DPA als Anhang 3 der Terms)	Brevo SAS, Paris – EWR; für DE/AT/CH Brevo GmbH, Berlin	Kein Drittland beim Vertragspartner	Widerspruch nur bei nachgewiesenem Verstoß (nicht neu gemessen)	brevo.com/legal/termsofuse (01.10.2025; Stand 27.11.2026)

Werkzeug	Tarif	Geschäftsnutzung im Gratistarif	AVV – Stufe und Weg	Vertragspartner · Region	Drittlandgrundlage	Stolperstein	Quelle, Stand
Mailgun / Mailjet (Sinch)	–	nicht gemessen	Sinch-DPA Teil des Hauptvertrags (V 8)	Mailgun: Region je Domain, **EU nur bei aktiver Wahl** (eigener Endpunkt) · Mailjet: Paris	SCC; DPF für Sinch Email	Region wird je Domain gewählt, nicht je Konto	mailgun.com/about/regions (09.11.2026); sinch.com DPA (V 8, 29.10.2025) (Stand 27.11.2026)
Simple Analytics nutze ich	Amsterdam	kein Free-Tarif	**Kein Standard-DPA** – „Simple Analytics does not process personal data. Because of this, a DPA is not required"; unterschreibt kundenseitige Vorlagen	Simple Analytics B.V., NL; Infrastruktur EU	Kein Drittland	„Keine personenbezogenen Daten" ist eine Anbieterposition – die IP-Adresse erreicht den Anbieter technisch trotzdem; wer einen AVV will, liefert die Vorlage	simpleanalytics.com/data-processing-agreement (ohne Datum; Stand 27.11.2026)
Plausible	Hosting EU	Testphase	**Automatisch** – „Use of the service constitutes acceptance of this DPA"	Europäische Gesellschaft (Sitz nicht genannt); Falkenstein (Hetzner), Finnland (UpCloud)	Kein Drittland	Vorfallmeldung „no later than 48 hours"; cookielos	plausible.io/dpa (November 2026)
Matomo	**Cloud**	Testphase	DPA existiert	**InnoCraft Ltd, Neuseeland** (Angemessenheitsbeschluss); Hosting AWS Frankfurt, Sicherungen Dublin	Angemessenheitsbeschluss NZ	EU-Hosting, Vertragspartner außerhalb der EU	matomo.org/matomo-cloud-dpa (Version 3.1, 20.11.2026)
Matomo	**On-Premise**	Ja (GPL)	Kein DPA mit Matomo (Matomo stellt keinen bereit) – AVV mit dem eigenen Hoster	Betreiber selbst	entfällt	Updates, IP-Kürzung, Cookie-Konfiguration liegen beim Betreiber	matomo.org FAQ 30990 (02.04.2026; Stand 27.11.2026)

Werkzeug	Tarif	Geschäftsnutzung im Gratistarif	AVV – Stufe und Weg	Vertragspartner · Region	Drittlandgrundlage	Stolperstein	Quelle, Stand
Google Analytics 4	–	Ja	Google Ads Data Processing Terms (V 8.0), per Klick in der Property zu akzeptieren	Google Ireland Ltd; Verarbeitung USA	SCC plus „Alternative Transfer Solution“ (DPF nicht namentlich genannt)	**Einwilligung erforderlich** (§ 25 TDDDG, Consent Mode v2); mehrere EU-Aufsichten hatten 2022/23 konkrete Einsätze für unzulässig erklärt – vor dem DPF	business.safety.google/adsprocessorterms (V 8.0, 30.05.2024; Stand 27.11.2026); DSK-Beschluss 26.05.2020; dr-datenschutz.de (sekundär)
GitHub nutze ich (nur für Code ohne personenbezogene Daten)	**Free / Pro (persönliches Konto)**	Ja	**Kein** DPA – der GitHub-DPA gilt für Enterprise Cloud, Teams und Copilot; die ToS für Free/Pro nennen keinen	GitHub, Inc., USA	nicht gemessen	Testdaten mit Kundennamen, Issues, .env-Dateien in einem Repo eines persönlichen Kontos: kein Art.-28-Vertrag	docs.github.com Terms of Service (27.04.2026); github.com/customer-terms/github-data-protection-agreement (Stand 27.11.2026)
GitHub	**Team / Enterprise Cloud**	Ja	DPA Bestandteil des Customer Agreement	wie oben; EU-Datenresidenz nur Enterprise mit Data Residency (nicht gemessen)	SCC (nicht gemessen)	Der Wechsel vom persönlichen Konto zur Organisation ist der Weg zum Vertrag	ebd. (Stand 27.11.2026)
GitLab.com	–	nicht gemessen	DPA existiert; Geltung je Tarif nicht gemessen	GitLab Inc., USA / GitLab B.V., NL (nicht gemessen)	nicht gemessen	–	about.gitlab.com/handbook/legal/data-processing-agreement · nicht neu gemessen (Stand 03.09.2026; DPA-Text am 27.11.2026 nicht erreicht)

C.6 E-MAIL, OFFICE, SPEICHER, ZUSAMMENARBEIT – DIE LEICHT ÜBERSEHENEN KANDIDATEN

Zur Transparenz: Werkzeuge mit dem Kennzeichen „nutze ich“ setze ich derzeit selbst ein.

Werkzeug	Tarif	Geschäftsnutzung im Gratis-/Verbrauchertarif	AVV	Vertragspartner · Region	KI-Funktionen und Datenverwendung	Stolperstein	Quelle, Stand
Gmail kostenlos (@gmail.com), Google Drive privat	–	Kein ausdrückliches Verbot gefunden; Google führt „business users“ in einen eigenen Vertrag (Workspace (Personal): „for business use“)	**Kein** AVV – nur die Google-Datenschutzerklärung, Google als eigener Verantwortlicher	Google Ireland Ltd; Region global	Gemini-Funktionen standardmäßig aktiv, abschaltbar; kein Training laut Google – als Aussage, nicht als Vertrag	**Der häufigste Negativkandidat.** Ausweg mit @gmail.com: Workspace (Personal), dort ist der DPA Vertragsbestandteil (Abschn. 1, 4)	workspace.google.com/terms/workspace-personal-terms (17.08.2026; Stand 27.11.2026); privacy.google.com/businesses/gdprprocessorterms und Gmail-Privatkonto (nicht neu gemessen, Stand 03.09.2026)
Google Workspace	–	Geschäftsprodukt	**Automatisch** (Cloud Data Processing Addendum)	Google Ireland Ltd; Datenregion je Edition	Vertragliche Zusage: kein Training außerhalb der Organisation	Gleiche Server, gleiche Oberfläche wie Gmail – der Unterschied ist ausschließlich vertraglich	workspace.google.com/security/ai-privacy (Stand 27.11.2026)
Outlook.com / Hotmail / Microsoft 365 Personal und Family	–	Microsoft-Servicevertrag selbst ohne eigenes Verbot für Outlook/Microsoft-365-Apps, verweist auf Zusatzbedingungen (nicht gelesen); Microsoft 365 Personal/Family laut Lizenzhinweis „personal, non-commercial“ (sekundär)	**Kein** DPA (Verbrauchervertrag)	Microsoft Ireland Operations Ltd; keine Regionszusage	nicht gemessen	„Microsoft 365“ heißt Verbraucher- und Geschäftsabo gleichermaßen	microsoft.com/servicesagreement (wirksam 30.09.2026; Stand 27.11.2026); learn.microsoft.com Q&A 5159668 (sekundär)

Werkzeug	Tarif	Geschäftsnutzung im Gratis-/Verbrauchertarif	AVV	Vertragspartner · Region	KI-Funktionen und Datenverwendung	Stolperstein	Quelle, Stand
Microsoft 365 Business	–	Geschäftsprodukt	Microsoft Products and Services DPA (Fassung 01.11.2026); automatische Geltung für M365 Business auf der DPA-Seite nicht ausdrücklich genannt	Microsoft Ireland; EU Data Boundary für Geschäftsdienste	Kein Training laut Product Terms	EU Data Boundary gilt nicht für Outlook.com	microsoft.com/licensing/docs DPA (01.11.2026; Stand 27.11.2026); learn.microsoft.com EU Data Boundary (nicht neu gemessen)
Apple iCloud / iCloud Mail / iCloud Drive	–	Für Privatgebrauch gedacht: „designed and intended for personal use“ (Abschn. IV.A)	**Kein** AVV in den iCloud-Bedingungen – einziges Art.-28-Dokument bei Apple ist der **Apple Business Manager Agreement** (Managed Apple Accounts)	Apple Distribution International Ltd, Cork; keine Regionszusage	Apple Intelligence siehe C.7	iCloud wird bei der Geräteeinrichtung automatisch aktiviert; „Schreibtisch & Dokumente“ landet in iCloud Drive. iCloud Mail nie Ende-zu-Ende-verschlüsselt, auch nicht mit erweitertem Datenschutz	apple.com/legal/internet-services/icloud/en/terms.html (14.09.2026; Stand 27.11.2026); apple.com/legal/enterprise/apple-business-manager/abm-us.pdf und support.apple.com ADP-Guide (nicht neu gemessen)
Proton Mail	**/ Proton for Business** Schweiz	Free: nicht gemessen	DPA für Business-Pläne (automatisch); Free nicht gemessen	Proton AG, Schweiz – Drittland mit Angemessenheitsbeschluss	Proton Scribe: nicht gemessen	Schweiz ist kein EWR	proton.me/legal/dpa (10.02.2026; Stand 27.11.2026); Free nicht neu gemessen
mailbox.org	Berlin	Privat- und Business-Tarife getrennt	**Per Klick** in der Accountverwaltung (Business-Konto)	Heinlein Hosting GmbH, DE	keine bekannt	–	mailbox.org; Heinlein-AVV (PDF 06/2022) · nicht neu gemessen (Stand 03.09.2026; Seite am 27.11.2026 nicht abrufbar)
Posteo	Berlin	keine Unterscheidung gefunden	**Nicht gemessen** – auf posteo.de keine AVV-Seite gefunden	Posteo e.K., DE	keine bekannt	Anonyme Anmeldung – für Geschäftskonten mit Rechnungsbedarf prüfen	posteo.de/site/terms (Stand 27.11.2026: weiterhin keine AVV-Seite gefunden)

Werkzeug	Tarif	Geschäftsnutzung im Gratis-/Verbrauchertarif	AVV	Vertragspartner · Region	KI-Funktionen und Datenverwendung	Stolperstein	Quelle, Stand
Dropbox	**Basic / Plus**	nicht gemessen	**Kein** DPA – der DPA „supplements the Dropbox Business Agreement"; auch der bezahlte Einzeltarif Plus hat keinen (Forum: Mindestgröße 3 Nutzer, sekundär)	Dropbox International Unlimited Company, Dublin	Dash/KI: nicht gemessen	Bezahlt heißt nicht kommerziell	dropbox.com/business_agreement (05.12.2024, neue Fassung ab 01.01.2027; Stand 27.11.2026); DPA-PDF (23.08.2024)
WeTransfer	**Free**	nicht untersagt	DPA „supported on paid business plans"	WeTransfer B.V., Amsterdam	2025: „machine learning"-Klausel eingeführt und nach Kritik gestrichen	Inhalte-Lizenzen in Gratisdiensten regelmäßig neu lesen	wetransfer.com Help Center; Blog Juli 2025 · nicht neu gemessen (Stand 03.09.2026)
Notion	**Free / Plus / Business**	nicht eingeschränkt gefunden	„A Data Processing Addendum is available for all customers"	Notion Labs, USA; EU-Residenz nur bestimmte Pläne	Notion AI: kein Training; LLM-Aufbewahrung 30 Tage außer Enterprise	–	notion.com/help/privacy; …/notion-ai-security-practices · nicht neu gemessen (Stand 03.09.2026; DPA-Seite am 27.11.2026 nicht abrufbar)
Slack	**Free / Pro**	Free für Geschäftsnutzung vorgesehen	DPA ergänzt die Customer Terms, Ausführung über DPA-Formular; Planabdeckung auf der Seite nicht genannt	Slack Technologies Ltd, Dublin	Nicht-generative „global models" mit Kundendaten; **Opt-out nur per E-Mail** an feedback@slack.com	Free zeigt 90 Tage und löscht Nachrichten nach einem Jahr – Nachweise gehen verloren	slack.com/terms-of-service/data-processing (Stand 27.11.2026); slack.com/trust privacy-principles (nicht neu gemessen)
Zoom	**Basic / Pro**	nicht untersagt	Global DPA „forms part of the … Terms of Service" – auch Basic	Zoom, USA; EU-Rechenzentren wählbar (nicht gemessen)	AI Companion: Ausschluss (siehe C.4)	–	media.zoom.com Global DPA · nicht neu gemessen (Stand 03.09.2026; Seite am 27.11.2026 nicht abrufbar)

Werkzeug	Tarif	Geschäftsnutzung im Gratis-/Verbraucherta-rif	AVV	Vertragspartner · Regi-on	KI-Funktionen und Da-tenverwendung	Stolperstein	Quelle, Stand
Calendly	**Free**	vorgesehen	DPA „incorporated into the Customer Terms“	Calendly LLC, Buford (USA); **Verarbeitung in den USA und wei-teren Ländern**, keine EU-Region	nicht gemessen	Kundennamen und -Mails eines KMU lie-gen bei einem US-An-bieter ohne EU-Regi-on	calendly.com/legal/data-processing-addendum (wirksam 01.06.2026; Stand 27.11.2026)
Trello Free · Asana Personal	–	vorgesehen	Atlassian-DPA auto-matisch mit dem Cu-stomer Agreement (Free nicht ausdrück-lich genannt) · Asana-DPA per Verweis in der Subscription Agree-ment (Personal nicht genannt)	Atlassian (Gesell-schaft nicht genannt) · Asana, Inc., USA	nicht gemessen	Atlassian: Wider-spruch nur in der 30-Tage-Mitteilungsfrist, Mitteilung nur an abonnierte Adressen	atlassian.com/legal/data-processing-addendum (17.08.2026); asana.com/terms/data-processing (01.09.2026) (beide Stand 27.11.2026)

C.7 BORDMITTEL VON MACOS UND IOS

Grundsatz für alle Zeilen: Mit einem privaten Apple-Account gilt der Verbrauchervertrag. Ein Art.-28-Regime bei Apple gibt es nur über Apple Business Manager mit Managed Apple Accounts (kostenlos, D-U-N-S-Nummer nötig).

Funktion	Verlässt der Inhalt das Gerät – und zu wem?	Zusage	Kontrolle	Quelle, Stand
Apple Intelligence, Verarbeitung auf dem Gerät	Nein, solange das Gerätemodell reicht: laut Apple läuft die Verarbeitung „in many cases" ganz auf dem Gerät; braucht eine Aufgabe mehr Rechenleistung, geht sie an Private Cloud Compute	Kein Training mit Inhalten; Geräteanalyse abschaltbar	Einstellungen › Datenschutz & Sicherheit › Analyse	apple.com/legal/privacy/data/en/intelligence-engine (14.09.2026; Stand 27.11.2026)
Private Cloud Compute (PCC)	Ja, zu Apple-Servern, wenn das Gerät es so entscheidet	„not stored or made accessible to Apple"; Apple erhebt nur Größe, Funktion, Dauer, nicht mit dem Account verknüpft	**Apple Intelligence & PCC Report** (Einstellungen › Datenschutz & Sicherheit) zeigt, was das Gerät verlassen hat; das einzige Messinstrument	ebd. (Stand 27.11.2026); PCC-Serverregion auf der Seite nicht genannt
ChatGPT-Integration (Siri, Schreibwerkzeuge, Visual Intelligence)	Ja, zu OpenAI – nur wenn aktiviert und je Anfrage bestätigt (Automatik einstellbar)	Ohne ChatGPT-Konto: OpenAI darf nur für die Anfrage verarbeiten, nicht speichern, IP verschleiert · **Mit verknüpftem Konto: OpenAIs Verbraucherbedingungen, Training möglich**	Ein verknüpftes Konto kippt den Vertrag von Apple zu OpenAI	apple.com/legal/privacy/data/en/chatgpt-extension (14.09.2026; Stand 27.11.2026)
Schreibwerkzeuge (Writing Tools)	Korrekturlesen/Umschreiben kann an PCC gehen; „Compose" via ChatGPT zu OpenAI	wie PCC bzw. ChatGPT	Wirkt in Drittanbieter-Apps – auch auf Kundentexte in Mail, Pages, Word	intelligence-engine (oben) · nicht neu gemessen (Stand 03.09.2026)
Diktat	Auf unterstützten Geräten und Sprachen vollständig offline; sonst Apple-Server	Audio nur bei Opt-in „Siri verbessern"	Siri-Einstellungen zeigen, ob lokal	apple.com/legal/privacy/data/en/ask-siri-dictation; Apple Newsroom 01/2025 · nicht neu gemessen (Stand 03.09.2026)
Sprachmemos, Notizen – Aufnahme und Transkription	Transkription lokal (sekundär); **Zusammenfassung** ist Apple Intelligence und kann an PCC gehen	wie PCC	Transkripte synchronisieren über iCloud	support.apple.com; get-inscribe.com (sekundär) · nicht neu gemessen (Stand 03.09.2026)

Funktion	Verlässt der Inhalt das Gerät – und zu wem?	Zusage	Kontrolle	Quelle, Stand
Apple Mail – Zusammenfassungen, Priorität	Vorschau-Zusammenfassungen lokal; Zusammenfassung einer geöffneten langen Mail kann an PCC gehen	wie PCC	**Betrifft auch geschäftliche IMAP-/Exchange-Konten in Apple Mail** – der Vertrag mit dem Mailanbieter deckt diese Verarbeitung nicht	intelligence-engine (oben) · nicht neu gemessen (Stand 03.09.2026)
iCloud-Synchronisation	Ja, zu Apple. Standard: 15 Kategorien Ende-zu-Ende, Schlüssel für den Rest bei Apple · **Erweiterter Datenschutz (ADP): Opt-in, nicht Standard**; 25 Kategorien	Apple kann Standard-geschützte Daten entschlüsseln (Behördenanfragen)	**Mail, Kontakte, Kalender bleiben auch mit ADP ohne Ende-zu-Ende-Schutz**	support.apple.com/102651 (05.01.2026; Stand 27.11.2026); support.apple.com/guide/security/sec973254c5f (nicht neu gemessen)

C.8 VERWALTUNG, BUCHHALTUNG, POST, SIGNATUR

Zur Transparenz: Werkzeuge mit dem Kennzeichen „nutze ich“ setze ich derzeit selbst ein.

Werkzeug	Tarif	AVV – Weg	Vertragspartner	Stolperstein	Quelle, Stand
Lexware Office (ehem. lexoffice) nutze ich	–	**Per Klick** in den Kontoeinstellungen („AVV gemäß Art. 28 DSGVO, den du direkt in den Einstellungen deines Accounts abschließen kannst“); AVV-Partner Haufe Service Center GmbH, Freiburg	Freiburg, DE	Ohne Klick liegt kein unterschriebener AVV vor – und ob geklickt wurde, weiß man nur, wenn man nachsieht	office.lexware.de AVV-PDF (26.03.2024); toolradar.de (sekundär) · nicht neu gemessen (Stand 03.09.2026; PDF am 27.11.2026 weiter auffindbar, Inhalt nicht neu gelesen)
sevdesk	–	Digital; AVV „muss nicht an uns versendet werden“ (Hilfeartikel 18.02.2026)	Offenburg, DE	AVV-PDF inkl. TOM öffentlich (14.07.2025; Datum nicht neu gemessen)	hilfe.sevdesk.de Artikel 9720486 (18.02.2026; Stand 27.11.2026)
DATEV Unternehmen online	–	**Gesondert**: Online-Zustimmung unter datev.de/av	DATEV eG, Nürnberg	DATEV ist Auftragsverarbeiter des Unternehmens **und** des Steuerberaters – der Steuerberater selbst ist keiner	datev.de Vereinbarung zur Auftragsverarbeitung; FAQ-PDF 2025 · nicht neu gemessen (Stand 03.09.2026; Seite am 27.11.2026 nicht abrufbar)
Dropscan nutze ich	Postdigitalisierung, Berlin	**Per Klick** in den Kontoeinstellungen unter „Datenschutz“ (gewerbliche Scanbox), elektronisch ohne Unterschrift	Dropscan GmbH, Berlin; Unterauftragsverarbeiter laut eigener Liste (nicht neu gemessen)	Post enthält fremde Personendaten; der Vertrag existiert erst mit dem Klick	dropscan.de/datenschutz/av-vertrag-vorlage (Vorlage „Stand November 2026“; Stand 27.11.2026); …/unterauftragsverarbeiter (nicht neu gemessen)
Caya	Berlin	AVV als Download auf der Compliance-Seite; ob für alle Tarife, nicht angegeben	Caya GmbH, Berlin; Hosting in Deutschland	–	caya.com/compliance (Stand 27.11.2026)
Docusign eSignature	**Web Plan**	**Automatisch** – Data Protection Attachment „incorporated into … the Terms“ (09.01.2025)	Docusign Inc., USA; EU-Kunden Docusign International (EMEA) Ltd, Dublin (nicht gemessen)	SCC „deemed signed“ plus Binding Corporate Rules	docusign.com/legal/terms-and-conditions/data-protection-attachment/web-plan (Stand 27.11.2026)

Werkzeug	Tarif	AVV – Weg	Vertragspartner	Stolperstein	Quelle, Stand
Adobe Acrobat Sign	**Einzelplatz**	DPA als Enterprise-PDF vorhanden; Geltung für Einzelabo **nicht gemessen**	Adobe Systems Software Ireland Ltd	Für ein Einzelabo nicht gemessen	adobe.com DPA-SCC-English_2022v2.pdf · nicht neu gemessen (Stand 03.09.2026)
Youtrust (ehem. Yousign)	Paris	**Automatisch**: DPA „forms an integral part of the Contract“ (Stand 02.07.2026)	Youtrust SAS, Frankreich; Hosting im DPA nicht genannt	Europäische Alternative ohne US-Mutter, eIDAS-qualifiziert (nicht neu gemessen)	youtrust.com/data-processing (02.07.2026; Stand 27.11.2026; yousign.com leitet dorthin um)
Banken, Steuerberater, Wirtschaftsprüfer, Rechtsanwälte, Versicherungen	–	**Kein AVV nötig** – eigene Verantwortliche (DSK-Kurzpapier Nr. 13: Berufsgeheimnisträger, Bankinstitute für den Geldtransfer, Postdienste)	–	Wer hier einen AVV verlangt, verwechselt Rollen; sie gehören ins Verarbeitungsverzeichnis als Empfänger	datenschutzkonferenz-online.de dsk_kpnr_13.pdf (17.12.2018; Stand 27.11.2026)

C.9 WO DIESER ANHANG WEISSE FLECKEN HAT

Damit niemand eine Lücke für eine Entwarnung hält: Das Folgende habe ich nicht messen können und deshalb nicht behauptet. Wer eines dieser Werkzeuge einsetzt, prüft genau diese Punkte selbst am Anbietertext – und wer mir eine Fundstelle schickt, hilft der nächsten Fassung.

Preise fast aller Tarife (Preisseiten laden per Skript oder regionalisiert); Microsoft-Zusatzbedingungen zur Geschäftsnutzung von Outlook.com und Microsoft 365 Personal (aka.ms/useterms); Google Workspace CDPA im Wortlaut; Perplexity- und xAI-Enterprise-Terms; aktuelle xAI-Verbraucherbedingungen; Netlify Free; Posteo-AVV; Adobe Acrobat Sign Einzelabo; Region der Private-Cloud-Compute-Server; Apple Business Manager Agreement in der EU-Fassung; Midjourney Privacy Policy im Volltext; Stability Community License im Volltext; alle als sekundär gekennzeichneten Angaben. Am 27.11.2026 außerdem nicht abrufbar oder nicht erneut aufgerufen und deshalb auf Stand 03.09.2026: IONOS, mailbox.org, Airtable, Notion-DPA, Zoom, Canva, DATEV, Lexware Office, WeTransfer, GitLab, AWS, Azure, Gmail-Privatkonto.

TEIL D

DIE DOKUMENTE UND RAHMENBEDINGUNGEN, DIE ICH GEBRAUCHT HABE

Keine Vollständigkeitsgarantie; die Liste ist das, was in meinem Betrieb angefallen ist – erledigt oder als offener Punkt mit Termin in der Akte. Die Spalte „Warum ich es brauchte“ beschreibt den Anlass, nicht den Erledigungsstand. Je Punkt: worum es geht, warum, und woran ich es festgemacht habe.

Nr.	Dokument / Rahmenbedingung	Worum es geht	Warum ich es brauchte	Fundstelle
1	**Auftragsverarbeitungsvertrag (AVV / DPA) je Dienst**	Vertrag mit jedem Dienst, der für mich personenbezogene Daten verarbeitet: nur auf Weisung, Sicherheitsmaßnahmen, Unterauftragnehmer nur mit Zustimmung, Löschung am Ende	Art. 28 Abs. 3 DSGVO verlangt ihn; ohne ihn fehlte mir die Grundlage – auch wenn der Anbieter „sicher“ ist. Bei KI-Anbietern nur in Geschäftstarifen; bei deutschen Diensten oft per Klick im Kundenportal	Art. 28 Abs. 3 DSGVO
2	**Nachweis, dass der AVV tatsächlich gilt**	Kopie oder Bestätigung: automatisch mit den AGB, per Klick ausgelöst, oder gegengezeichnet – mit Datum	Die Rechenschaftspflicht verlangt den Nachweis, nicht die Annahme	Art. 5 Abs. 2 DSGVO
3	**Verzeichnis der Verarbeitungstätigkeiten (VVT)**	Liste aller Verarbeitungen: Zweck, Datenkategorien, Betroffene, Empfänger, Drittland, Löschfrist, Schutzmaßnahmen	Die Ausnahme für Betriebe unter 250 Beschäftigten greift praktisch nie; jedes KI-Werkzeug gehört in die betroffenen Verarbeitungstätigkeiten	Art. 30 DSGVO; DSK-Kurzpapier Nr. 1
4	**Datenschutzerklärung (Website, Kunden)**	Nennt Anbieter als Empfänger, Drittlandübermittlung und deren Grundlage, Speicherdauer	Ein KI-Werkzeug mit Kundendaten, das dort nicht steht, ist ein Transparenzverstoß – der Reverse Proxy und der Hoster gehören dazu	Art. 13, 14 DSGVO
5	**Drittlandgrundlage je Dienst**	DPF-Zertifizierung des Empfängers (prüfbar unter dataprivacyframework.gov) oder Standardvertragsklauseln im Vertrag; bei SCC ein Transfer Impact Assessment	Auch der Fernzugriff aus einem Drittland zählt als Übermittlung; „Server in Frankfurt“ allein genügt nicht, wenn der Vertragspartner in Singapur sitzt	Art. 44–46 DSGVO; Durchführungsbeschlüsse 2023/1795 und 2021/914
6	**Abonnement der Unterauftragsverarbeiter-Benachrichtigung**	Eintrag in die Benachrichtigungsliste jedes Anbieters	Ohne Eintrag läuft die Widerspruchsfrist (5 bis 30 Tage) ins Leere	Art. 28 Abs. 2, 4 DSGVO; jeweiliger DPA
7	**Technische und organisatorische Maßnahmen (TOM)**	Eigene Maßnahmen: Zwei-Faktor, Rollen im Teamkonto, Historie und Training aus, Regel zum Entfernen von Namen vor der Eingabe, schriftliche Nutzungsanweisung	Müssen zum Risiko passen und im VVT und AVV beschrieben sein	Art. 32 DSGVO; DSK-Orientierungshilfe KI-Systeme (17.06.2025)
8	**Interne Werkzeugregel („die fünf Nebenwege“)**	Was in welches Werkzeug darf – Produktivdaten nie in ein Verbraucherwerkzeug; Anonymisierung statt Pseudonymisierung	Der Regelungsbedarf, den kein Tarif löst; kostet nichts	Art. 4 Nr. 5, Art. 6 Abs. 4 DSGVO
9	**Kurzanweisung KI-Kompetenz**	Eine Seite: was darf hinein, was nicht, wie wird geprüft, wie gekennzeichnet; Datum, Einweisung, Ablage	Betreiberpflicht seit 02.02.2025; kein Zertifikat, keine Schulungsform vorgeschrieben	Art. 4 KI-VO (Fassung nach VO (EU) 2026/1744)

Nr.	Dokument / Rahmenbedingung	Worum es geht	Warum ich es brauchte	Fundstelle
10	**Vorabprüfung Datenschutz-Folgenabschätzung**	Dokumentierte Antwort auf die Frage, ob eine DSFA nötig ist – bei einem Kunden-Chatbot: ja	Steht auf der Muss-Liste der deutschen Aufsicht (Nr. 11); auch das Nein gehört in die Akte	Art. 35 DSGVO; DSK-Liste Art. 35 Abs. 4, Nr. 11
11	**Hinweisblatt und Einwilligung für Gesprächsaufzeichnung**	Information nach Art. 13 plus Einwilligung jedes Sprechenden vor der Aufnahme; Verfahren beschrieben (lokal, Bereinigung, dann KI); Widerruf; Löschfristen	Aufnahme ohne Einwilligung ist strafbar; der Plattformhinweis genügt nicht; bei Coaching ausdrückliche Einwilligung	§ 201 StGB; Art. 6 Abs. 1 lit. a, Art. 7, Art. 9 Abs. 2 lit. a DSGVO
12	**Protokoll je Aufzeichnung**	Eine Zeile je Gespräch: Teilnehmer, Form der Einwilligung, Beleg, Werkzeuge, Speicherort, Bereinigung, Löschung	Nachweis nach Art. 7 Abs. 1; die zugesagte Löschung muss stattfinden	Art. 7 Abs. 1 DSGVO
13	**Kundenvertrag: Klauseln zu KI-Werkzeugen**	Zusage, nur Werkzeuge mit vertraglichem Trainingsausschluss zu nutzen; Vertraulichkeit; Umgang mit Erfahrungswissen; AVV zwischen Kunde und Berater, wenn der Berater Daten der Kundenmitarbeiter im Auftrag verarbeitet	Was ich meinem Kunden zusage, muss der gewählte Tarif halten – mein Verbraucherabo hielt es nicht	§ 2 GeschGehG; Art. 28 DSGVO (Gegenrichtung)
14	**Bildnachweis und Kennzeichnung KI-erzeugter Inhalte**	Satz im Bildnachweis; sichtbare Offenlegung bei Deepfakes; Regel im Bild-Styleguide, wo die Grenze kippt (reale Person, realer Ort, fotorealistisch, als Tatsachennachweis)	Betreiberpflicht seit 02.08.2026; Anbietermarkierung genügt nicht; zusätzlich § 5 UWG	Art. 50 Abs. 4, Art. 3 Nr. 60 KI-VO; § 5 UWG
15	**Löschkonzept**	Fristen je Datenart: Tonaufnahme, Rohtranskript, Chatverläufe, Logs, Anwendungsdaten	Speicherbegrenzung; Zusagen in Hinweisblatt und Datenschutzerklärung müssen stimmen	Art. 5 Abs. 1 lit. e DSGVO
16	**Aufbewahrung nach Steuer- und Handelsrecht**	Belege im Originalformat GoBD-gerecht aufbewahren (Papier oder zulässig ersetzend gescannt); KI-Ausgaben ersetzen sie nicht; eine KI-generierte Auftragsbestätigung ist ein Handelsbrief	8 Jahre Buchungsbelege (seit 01.01.2025), 10 Jahre Bücher, 6 Jahre Geschäftsbriefe; GoBD-Verfahrensdokumentation	§ 147 AO; GoBD (BMF 28.11.2019, geändert 11.03.2024)
17	**Akte mit Datum, Messung, Beleg**	Je Werkzeug: was wann gemessen wurde, welche Entscheidung folgte, mit Herkunftsvermerk	Nachweis der Bemühung – im Ernstfall der Unterschied zwischen lit. b und lit. c, f, h	Art. 83 Abs. 2 DSGVO
18	**Verpflichtung als „mitwirkende Person“**, wenn man für Berufsgeheimnisträger arbeitet	Schriftliche Verpflichtung zur Verschwiegenheit durch den Auftraggeber; eigene Strafbarkeit; kein Werkzeug mit Trainingsrecht für Mandanten- oder Patientendaten	Wer für Ärzte, Anwälte, Steuerberater arbeitet, steht unter demselben Geheimnisschutz	§ 203 Abs. 3, 4 StGB; § 43e BRAO; § 62a StBerG
19	**Einwilligung für Chat-Widgets und Analyse auf der Website**	Einwilligung, bevor ein KI-Chat-Widget oder eine Analyse auf das Endgerät zugreift, soweit das nicht unbedingt erforderlich ist	Zugriff auf das Endgerät ist einwilligungspflichtig, außer er ist unbedingt erforderlich	§ 25 TDDDG

TEIL E

LEXIKON

Kurz und in der Reihenfolge, in der die Begriffe mir begegnet sind. Fundstellen im Quellenverzeichnis.

Consumer Terms / Commercial Terms

Die zwei Vertragswelten jedes großen KI-Anbieters. Consumer Terms (Privatkonto: Free, Plus, Pro, Max): Der Nutzer ist Verbraucher, es gibt keinen AVV, Eingaben dürfen in der Regel zum Training verwendet werden (Opt-out möglich), Gerichtsstand je nach Fassung USA oder EU. Commercial Terms (Team, Enterprise, API): Der Kunde ist Unternehmer, es gibt ein DPA mit SCC oder DPF, Training ist vertraglich ausgeschlossen (in der Regel; Ausnahmen je Anbieter, siehe Anhang), Fristen sind definiert. Gleiche Oberfläche, anderer Vertrag – der Tarif entscheidet.

AVV / DPA (Auftragsverarbeitungsvertrag / Data Processing Addendum)

Der Vertrag nach Art. 28 Abs. 3 DSGVO zwischen dem Unternehmen (Verantwortlicher) und dem Dienstleister (Auftragsverarbeiter). Legt fest, dass der Dienstleister nur auf Weisung verarbeitet, Sicherheitsmaßnahmen trifft, Unterauftragnehmer nur mit Genehmigung einsetzt (einzeln oder allgemein mit Widerspruchsrecht) und Daten am Ende löscht. Bei KI-Anbietern meist „Data Processing Addendum“ und meist nur in Geschäftstarifen; andere Dienste bieten ihn teils allen Kunden an.

Verantwortlicher

Wer über Zwecke und Mittel der Verarbeitung entscheidet (Art. 4 Nr. 7 DSGVO) – das Unternehmen, das ein Werkzeug auswählt und Kundendaten eingibt. Trägt die Rechenschaft, informiert die Betroffenen, haftet für Bußgelder.

Auftragsverarbeiter

Wer im Auftrag und weisungsgebunden verarbeitet, ohne eigene Zwecke (Art. 4 Nr. 8). Ein KI-Anbieter ist Auftragsverarbeiter nur für die Vorgänge, die er allein im Auftrag ausführt. Nutzt er Eingaben für eigene Zwecke – etwa Training –, ist er insoweit selbst Verantwortlicher, und man übermittelt an einen Dritten.

Unterauftragsverarbeiter (Subprozessor)

Dienstleister des Dienstleisters – typischerweise Cloud-Rechenzentrum, Support, Zahlungsabwickler. Darf nur mit Genehmigung eingesetzt werden; bei allgemeiner Genehmigung muss man über Änderungen informiert werden und widersprechen können (Art. 28 Abs. 2, 4). Die Subprozessorliste zeigt, wo die Daten wirklich liegen.

Gemeinsame Verantwortlichkeit

Zwei Stellen legen Zwecke und Mittel gemeinsam fest (Art. 26). Kommt vor, wenn Anbieter und Nutzer gemeinsam über Zweck und wesentliche Mittel entscheiden, etwa wenn Berater und Kunde einen Chatbot gemeinsam konzipieren und betreiben; braucht eine Vereinbarung, wer welche Pflicht erfüllt.

Standardvertragsklauseln (SCC)

Von der Kommission genehmigte Klauseln (Durchführungsbeschluss (EU) 2021/914) für Übermittlungen in Drittländer, in vier Modulen. Dürfen nicht verändert werden; verlangen ein Transfer Impact Assessment.

1. Verantwortlicher an Verantwortlichen
2. Verantwortlicher an Auftragsverarbeiter (der Normalfall: Unternehmen an US-Anbieter)
3. Auftragsverarbeiter an Unterauftragsverarbeiter
4. Auftragsverarbeiter an Verantwortlichen

Data Privacy Framework (DPF)

Der Angemessenheitsbeschluss der Kommission für die USA (Durchführungsbeschluss (EU) 2023/1795 vom 10.07.2023). Erlaubt Übermittlungen an US-Unternehmen, die sich beim US-Handelsministerium zertifiziert haben – ohne SCC und TIA, aber nur für gelistete Empfänger und Datenkategorien. Stand 03.09.2026: gültig; Klage abgewiesen (EuG T-553/23), Rechtsmittel beim EuGH (C-703/25 P); nach dem US-Supreme-Court-Urteil vom 29.06.2026 zur FTC-Unabhängigkeit haben noyb und der Europäische Datenschutzausschuss die Kommission zur Prüfung aufgefordert.

Transfer Impact Assessment (TIA)

Die dokumentierte Prüfung, ob Recht oder Praxis des Ziellands die Garantien der SCC praktisch aushebeln, und welche Zusatzmaßnahmen das ausgleichen. Pflicht bei SCC seit EuGH Schrems II (C-311/18); bei DPF-zertifizierten Empfängern formal nicht nötig.

EU-Datenresidenz gegen EU-Vertragspartner gegen EU-Verarbeitung

Drei verschiedene Dinge: wo die Daten liegen; mit wem der Vertrag besteht; wo gerechnet wird und wer zugreift. Jedes allein löst das Drittlandproblem nicht. Eine EU-Tochter eines US-Konzerns kann über die Mutter US-Zugriffsbefugnissen ausgesetzt sein; EU-Speicherung hilft nicht, wenn Support oder Missbrauchsprüfung aus den USA zugreifen.

Trainingsausschluss: Opt-out gegen vertraglich

Ein Opt-out ist ein Schalter im Verbraucherkonto, den der Anbieter jederzeit ändern kann. Ein vertraglicher Ausschluss steht im DPA oder in den Commercial Terms und ist einklagbar. Nur der vertragliche macht den Anbieter zum reinen Auftragsverarbeiter und schützt Geschäftsgeheimnisse.

Zero Data Retention (ZDR)

Zusage des Anbieters, Ein- und Ausgaben nach der Verarbeitung nicht zu speichern – auch nicht die 30 Tage Missbrauchskontrolle, die viele Schnittstellen als Standard haben. Ein Anbieterbegriff, kein Rechtsbegriff; bei den großen Anbietern ein Antrag, kein Häkchen, und nicht für jedes Modell verfügbar.

Technische und organisatorische Maßnahmen (TOM)

Alle Schutzmaßnahmen nach Art. 32: technisch (Verschlüsselung, Zugriffskontrolle, Zwei-Faktor, Löschroutinen) und organisatorisch (Richtlinie, Einweisung, Vertraulichkeitsverpflichtung). Prüfpunkt beim Anbieter: Anhang des Vertrags oder Beschreibung auf einer Webseite?

Verzeichnis der Verarbeitungstätigkeiten (VVT)

Die Liste aller Verarbeitungen nach Art. 30 mit Zweck, Datenkategorien, Betroffenen, Empfängern, Drittland, Löschfrist, TOM. Die Ausnahme für unter 250 Beschäftigte greift laut Aufsicht praktisch nie.

Datenschutz-Folgenabschätzung (DSFA)

Die vorab dokumentierte Risikoanalyse nach Art. 35 für Verarbeitungen mit voraussichtlich hohem Risiko. Pflicht bei allem auf der „Muss-Liste“ der deutschen Aufsicht – dort Nr. 11: KI zur Steuerung der Interaktion mit Betroffenen oder zur Bewertung persönlicher Aspekte.

Einwilligung

Freiwillige, informierte, unmissverständliche Willensbekundung für einen bestimmten Fall (Art. 4 Nr. 11, Art. 7): nachweisbar, jederzeit widerrufbar, bei Art.-9-Daten ausdrücklich. Kein AGB-Satz, kein vorangekreuztes Kästchen. Für den KI-Einsatz gegenüber Kunden oft die schwächste Grundlage, weil der Widerruf den Prozess stoppt; unverzichtbar bei Aufnahmen.

Berechtigtes Interesse

Rechtsgrundlage nach Art. 6 Abs. 1 lit. f: dreistufiger Test (Interesse, Erforderlichkeit, Abwägung), dokumentiert, mit Widerspruchsrecht. Für „KI hilft beim Antworten auf Kundenmails“ die übliche Grundlage neben der Vertragserfüllung. Nie für Art.-9-Daten.

Zweckänderung

Daten, die für Zweck A erhoben wurden (Kundenservice), für Zweck B verwenden (Testdaten, Training) – nur zulässig, wenn die Zwecke vereinbar sind (Art. 6 Abs. 4). Die Norm, an der Produktivdaten als Testdaten meist scheitern.

Anonymisierung gegen Pseudonymisierung

Pseudonymisierung ersetzt Identifikatoren und hält den Schlüssel getrennt – die Daten bleiben personenbezogen (Art. 4 Nr. 5). Anonymisierung entfernt den Personenbezug so, dass niemand mit vernünftigen Mitteln die Person bestimmen kann – dann gilt die DSGVO nicht. „Name durch Kunde A ersetzt" ist Pseudonymisierung; Adresse, Fall und Datum identifizieren oft trotzdem (EDSA-Leitlinien 02/2026: keine Herauslösung, keine Verknüpfung, keine Ableitung).

Anbieter und Betreiber (KI-Verordnung)

Anbieter (Art. 3 Nr. 3) entwickelt und bringt unter eigenem Namen in Verkehr; Betreiber (Art. 3 Nr. 4) verwendet beruflich in eigener Verantwortung. Der Anbieter trägt Produkt- und Markierungspflichten, der Betreiber Kompetenz, Nutzung nach Anleitung und Offenlegung von Deepfakes. Wer ein Fremdmodell unter eigener Marke wesentlich verändert oder ein Modell selbst betreibt und unter eigenem Namen anbietet, kann Anbieter werden (Art. 25).

GPAI-Modell

KI-Modell mit allgemeinem Verwendungszweck (Art. 3 Nr. 63) – GPT, Claude, Gemini, Llama, Mistral. Deren Anbieter haben seit 02.08.2025 eigene Pflichten (Art. 53: Dokumentation, Urheberrechts-Policy, Zusammenfassung der Trainingsdaten). Für Nutzer keine eigene Pflicht, aber ein Prüfhebel.

Deepfake

KI-erzeugter oder manipulierter Bild-, Ton- oder Videoinhalt, der realen Personen, Orten oder Ereignissen ähnelt und fälschlich als echt erscheinen würde (Art. 3 Nr. 60). Täuschungsabsicht ist nicht Voraussetzung. Betreiber müssen offenlegen (Art. 50 Abs. 4).

Berufsgeheimnis

Die strafrechtlich geschützte Verschwiegenheit von Ärzten, Anwälten, Steuerberatern und anderen (§ 203 StGB). Externe dürfen einbezogen werden, wenn erforderlich und schriftlich verpflichtet – und sind dann selbst strafbar bei Offenbarung. Ein Anbieter mit Trainingsrecht ist für Mandanten- und Patientendaten praktisch nicht verpflichtbar; ich schließe ihn dafür aus.

Geschäftsgeheimnis

Information, die nicht allgemein bekannt, wirtschaftlich wertvoll und Gegenstand angemessener Geheimhaltungsmaßnahmen ist (§ 2 Nr. 1 GeschGehG). Der Schutz entsteht nur durch eigenes Tun – wer Kalkulationen in ein Werkzeug mit Trainingsrecht gibt, gefährdet den Schutz.

Rechtsdienstleistung

Jede Tätigkeit in konkreten fremden Angelegenheiten, die eine rechtliche Prüfung des Einzelfalls erfordert (§ 2 Abs. 1 RDG); ohne Erlaubnis verboten (§ 3). Erlaubt: die an die Allgemeinheit gerichtete Darstellung von Rechtsfragen (§ 2 Abs. 3 Nr. 5) – dieser Text – und Nebenleistungen zum eigenen Beruf (§ 5). Nicht erlaubt: „Bei Ihnen ist das rechtlich in Ordnung."

TEIL F

QUELLEN

Anbieterquellen abgerufen am 27.11.2026, soweit im Anhang nicht anders vermerkt. Rechtsakte in der konsolidierten Fassung auf EUR-Lex bzw. gesetze-im-internet.de; deutsche Normtexte wurden am Abruftag über den verwendeten Weg nicht ausgeliefert und sind aus dem Gesetzesstand wiedergegeben.

Rechtsakte und Behörden

1. DSGVO (VO (EU) 2016/679): eur-lex.europa.eu/eli/reg/2016/679/oj/deu
2. KI-Verordnung (VO (EU) 2024/1689): eur-lex.europa.eu/eli/reg/2024/1689/oj/deu · Änderung „Digital Omnibus on AI" (VO (EU) 2026/1744, in Kraft 27.07.2026): eur-lex.europa.eu/eli/reg/2026/1744/oj · Rat, PM 299/26 (07.05.2026) · White & Case, „EU AI Omnibus enters into force" (04.08.2026)
3. EU-Kommission: FAQ Art. 50 (Stand 24.07.2026), digital-strategy.ec.europa.eu/en/faqs/transparency-obligations-under-article-50-ai-act · Leitlinien Transparenz (20.07.2026) · Verhaltenskodex KI-erzeugte Inhalte (10.06.2026) · AI Act Service Desk, Art. 4
4. Angemessenheitsbeschluss EU-US DPF (Durchführungsbeschluss (EU) 2023/1795): eur-lex.europa.eu/eli/dec_impl/2023/1795/oj · SCC (Durchführungsbeschluss (EU) 2021/914): eur-lex.europa.eu/eli/dec_impl/2021/914/oj · EDSA Recommendations 01/2020 · noyb-Schreiben 30.06.2026 · EDSA-Schreiben 31.07.2026 (Ares(2026)7540711, Sekundärbericht ppc.land)
5. DSK: Orientierungshilfe KI und Datenschutz (06.05.2024) · OH KI-Systeme/TOM (17.06.2025) · OH RAG (10/2025) · Kurzpapier Nr. 1 (VVT) · Kurzpapier Nr. 13 (Auftragsverarbeitung, 17.12.2018) · Liste Art. 35 Abs. 4, nicht-öffentlicher Bereich, Version 1.1 (17.10.2018), Seite 7 Nr. 11 · Beschluss Google Analytics (26.05.2020)
6. EDSA: Opinion 28/2024 (17.12.2024) · Leitlinien 01/2025 Pseudonymisierung · 02/2026 Anonymisierung (07.07.2026) · 03/2026 Web Scraping (07.07.2026)
7. HmbBfDI, Diskussionspapier LLM (15.07.2024) · BlnBDI Jahresbericht 2024 · BfDI Handreichung KI (12/2025) · CNIL, Recommandations IA (2024–2025)
8. Deutsche Normen: § 201, § 203 StGB · § 2 Abs. 2 UrhG · § 2 GeschGehG · § 5 UWG · § 2, § 3, § 5 RDG · § 147 AO; GoBD (BMF 28.11.2019, geändert 11.03.2024) · § 25 TDDDG
9. US Supreme Court, Nichtannahme Thaler v. Perlmutter (02.03.2026; Sekundärberichte Mayer Brown, Finnegan)

Anbieter (Auswahl; vollständige Fundstellen in den Tabellen von Teil C)

1. Anthropic: anthropic.com/legal/consumer-terms (EWR- und US-Fassung, 08.10.2025) · anthropic.com/legal/commercial-terms (17.06.2025) · anthropic.com/legal/data-processing-addendum (24.02.2025) · claude.com/pricing · claude.com/regional-compliance · privacy.claude.com Artikel 10023580 und 7996866 · code.claude.com/docs/en/data-usage

2. OpenAI: openai.com/policies/eu-terms-of-use (16.01.2026) · openai.com/policies/services-agreement (01.01.2026) · openai.com/policies/data-processing-addendum (01.01.2026) · openai.com/enterprise-privacy (08.01.2026) · openai.com/policies/how-your-data-is-used-to-improve-model-performance (13.03.2026) · openai.com/policies/row-terms-of-use (01.01.2026) · developers.openai.com/api/docs/guides/your-data
3. Google: ai.google.dev/gemini-api/terms (wirksam 23.03.2026, aktualisiert 28.04.2026) · support.google.com/gemini/answer/13594961 (24.11.2026) · workspace.google.com/terms/workspace-personal-terms (17.08.2026) · workspace.google.com/security/ai-privacy · privacy.google.com/businesses/gdprprocessorterms
4. Microsoft: learn.microsoft.com/microsoft-365/copilot/microsoft-365-copilot-privacy (03.11.2026) · learn.microsoft.com/azure/foundry/responsible-ai/openai/data-privacy (05.06.2026) · learn.microsoft.com/privacy/eudb · microsoft.com/servicesagreement (30.09.2026) · Microsoft Products and Services DPA (01.11.2026) · Message Center MC1269223 (Flex Routing, sekundär)
5. Mistral: legal.mistral.ai/terms/data-processing-addendum (27.07.2026) · legal.mistral.ai/terms/commercial-terms-of-service (25.09.2026) · EU-Verbraucherbedingungen auf legal.mistral.ai (08.10.2026)
6. Perplexity: perplexity.ai/hub/legal/terms-of-service (23.01.2026; neue Fassung wirksam 01.01.2027) · DeepSeek: cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html (10.02.2026) · xAI: x.ai/legal/terms-of-service (01.09.2026, nicht neu gemessen)
7. AWS: docs.aws.amazon.com/bedrock (data-protection, abuse-detection) · GitHub: docs.github.com Copilot manage-policies; Terms of Service (27.04.2026); github.com/customer-terms/github-data-protection-agreement · Cursor: cursor.com/data-use (03.09.2026)
8. Midjourney: docs.midjourney.com Terms of Service (27.05.2026), Plan-Vergleich · Adobe: business.adobe.com Firefly AI approach · Canva: canva.com/safe-ai-canva-shield · Stability: stability.ai/license · Ideogram: ideogram.ai/licensing
9. MacWhisper: docs.macwhisper.com Artikel 52 · Otter: otter.ai/privacy-security · Fireflies: fireflies.ai/security · tl;dv: tldv.io/privacy · Zoom: media.zoom.com Global DPA · Plaud: support.plaud.ai; plaud.ai Privacy (21.11.2026) · Notion: notion.com/help/ai-meeting-notes; …/privacy; …/notion-ai-security-practices
10. Vercel: vercel.com/legal/terms (19.10.2026); vercel.com/docs/plans/hobby (12.11.2026); vercel.com/legal/dpa (17.03.2026) · Netlify: netlify.com/legal/terms-of-use (14.10.2026) · Cloudflare: cloudflare.com/cloudflare-customer-dpa (v6.4, 03.04.2026); cloudflare.com/terms · Supabase: supabase.com/legal/customer-resources/data-processing-addendum (Version 1, 01.08.2026) · netcup Helpcenter Auftragsverarbeitung · Hetzner Datenschutz-FAQ; accounts.hetzner.com/account/dpa · Strato: strato.de/agb/avv (V 3.5, 18.03.2024) · Railway: railway.com/legal/dpa · Airtable: support.airtable.com Artikel 4245698629 · Neon, MongoDB, AWS, Azure, GCP: siehe Teil C
11. Resend: resend.com/legal/dpa (Seitenstand 31.12.2025) · Postmark: postmarkapp.com/dpa (17.11.2025) · Brevo: brevo.com/legal/termsofuse (01.10.2025) · Mailgun: mailgun.com/about/regions · Simple Analytics: simpleanalytics.com/data-processing-agreement · Plausible: plausible.io/dpa (11/2026) · Matomo: matomo.org/matomo-cloud-dpa (Version 3.1, 20.11.2026); FAQ 30990 (02.04.2026)

12. Apple: apple.com/legal/internet-services/icloud/en/terms.html (14.09.2026) · apple.com/legal/privacy/data/en/intelligence-engine (14.09.2026) · apple.com/legal/privacy/data/en/chatgpt-extension (14.09.2026) · apple.com/legal/privacy/data/en/ask-siri-dictation · support.apple.com/102651 (05.01.2026) · support.apple.com/guide/security/sec973254c5f · apple.com/legal/enterprise/apple-business-manager/abm-us.pdf
13. Proton: proton.me/legal/dpa (10.02.2026) · mailbox.org · Posteo: posteo.de/site/terms · Dropbox: dropbox.com/business_agreement (05.12.2024, neue Fassung ab 01.01.2027); DPA-PDF (23.08.2024) · WeTransfer: Help Center; Blog Juli 2025 · Slack: slack.com/terms-of-service/data-processing; slack.com/trust privacy-principles · Calendly: calendly.com/legal/data-processing-addendum (01.06.2026) · Atlassian: atlassian.com/legal/data-processing-addendum (17.08.2026) · Asana: asana.com/terms/data-processing (01.09.2026)
14. Lexware Office: office.lexware.de AVV-PDF (26.03.2024) · sevdesk: hilfe.sevdesk.de Artikel 9720486 (18.02.2026) · DATEV: datev.de/av; FAQ-PDF 2025 · Dropscan: dropscan.de/datenschutz/av-vertrag-vorlage (Stand November 2026) · Caya: caya.com/compliance · Docusign: docusign.com/legal Data Protection Attachment Web Plan (09.01.2025) · Adobe Sign: DPA-SCC-English_2022v2.pdf · Youtrust (ehem. Yousign): youtrust.com/data-processing (02.07.2026)
15. Fremddiskussion zur Non-commercial-Klausel: Hacker News, Thread 47320526 (Frühjahr 2026)
16. Eigene frühere Beiträge: LinkedIn, „ChatGPT im deutschen Rechtsrahmen“ (14.05.2023), „KI in Deutschland und der EU – ein Wegweiser“ (20.05.2023), „Chat with the EU AI Act“ (16.06.2023)



Andreas Riedel baut digitale Produkte, investiert in Gründer und begleitet Teams und Führungskräfte; er ist Geschäftsführer der Wawayaro GmbH, Berlin. Dieser Text ist ein Erfahrungsbericht und ersetzt keine Rechtsberatung im Einzelfall. Entstanden im Dialog mit Claude (Anthropic): Recherche, Gliederung und Formulierung KI-gestützt; Prüfung, Entscheidungen und Verantwortung: Andreas Riedel. Herausgeberin: Wawayaro GmbH, Mörchinger Straße 36, 14169 Berlin, Amtsgericht Charlottenburg HRB 167179 B. Illustrationen, soweit vorhanden, KI-erzeugt (Anbieter im Bildnachweis).

Wawayaro GmbH · Mörchinger Str. 36 · 14169 Berlin · Fassung 4 · Stand 28.11.2026