Anleitung zur Umsetzung Ihrer DSGVO-Compliance bei Nutzung von Hedy AI

An: Kunden (Verantwortliche) von Hedy AI LLC Stand: 12.11.2025

Sehr geehrte Kundin, sehr geehrter Kunde,

Hedy AI LLC hat die notwendigen vertraglichen Grundlagen (AVV/DPA, SCC + TIA, TOMs, Sub-Prozessor-Liste) geschaffen, um Ihnen eine DSGVO-konforme Nutzung zu *ermöglichen*.

Um die Dienste von Hedy AI LLC im Sinne der EU-Datenschutz-Grundverordnung (DSGVO) datenschutzkonform *zu nutzen*, müssen Sie als Verantwortlicher Ihre eigenen Prüfungs- und Dokumentationspflichten (Rechenschaftspflichten gemäß Art. 5 Abs. 2 DSGVO) erfüllen.

Diese Anleitung dient als Checkliste für die Schritte, die Sie nun *Ihrerseits* durchführen und dokumentieren müssen.

Hinweis

Diese Anleitung wurde als Vorschlag erstellt, um Sie bei der Erfüllung Ihrer gesetzlichen Pflichten zu unterstützen. Sie ist jedoch keine individuelle Rechtsberatung und ersetzt nicht Ihre eigene, sorgfältige Prüfung, Implementierung und Dokumentation der Einhaltung der DSGVO wie z.B. das Verarbeitungsverzeichnis, die Datenschutzerklärung oder die Betroffenenrechte.

Bitte denken Sie bei Ihrer Compliance für Ihren spezifischen Anwendungsfall auch an weitere anwendbare EU- oder mitgliedstaatliche Gesetze wie z.B. die KI-Verordnung der EU, den EU Data Act,), etwaige branchen-spezifische Datenschutzvorschriften oder das Strafgesetzbuch sowie an berufsrechtliche Schweigepflichten oder Sicherheitsanforderungen.

Voraussetzungen + Kontext

Die Checkliste geht davon aus, dass Sie Ihre ersten datenschutz-rechtlichen Pflichten erfüllt haben und zu dem Schluss gekommen sind, dass Sie die Daten mit Hedy verarbeiten dürfen, d.h.

- **Sie haben einen legalen Zweck für die Verarbeitung definiert.**
- **Sie haben eine gültige Rechtsgrundlage nach Artikel 6 DSGVO für die Verarbeitung** (z.B. Vertragserfüllung, berechtigtes Interesse oder eine Einwilligung).
- **Es gibt KEIN hohes Risiko für Rechte und Freiheiten natürlicher Personen,** d.h. es ist entweder nach erster Prüfung keine Datenschutzfolgenabschätzung (DSFA) gemäß Art. 35 DSGVO notwendig oder Sie haben eine DSFA durchgeführt und kommen zu dem Ergebnis, dass Sie die Daten verarbeiten dürfen.
- **Sie verarbeiten KEINE besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO,** z.B. Gesundheitsdaten, Daten zur ethnischen Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit. Alternativ

können Sie die notwendigen erhöhten Sorgfaltspflichten durch eine DSFA sowie kritische Prüfungen bei TIA/TOMs/Subprozessoren nachweisen.

Sofern Sie sich bei einem dieser Punkte nicht sicher sind, empfehlen wir Ihnen, Ihren Datenschützer zu konsultieren. Bei Bedarf können wir Ihnen gerne einen Datenschützer nennen.

Checkliste: Ihre Schritte zur DSGVO-Compliance

Die in dieser Checkliste genannten Dokumente und Anhänge können Sie als Kunde von Hedy einsehen, indem Sie in den App-Einstellungen auf den Link "Trust Center" klicken. Sofern Sie noch nicht Kunde sind, können Sie Zugang zu den Dokumenten unter trust.hedy.ai beantragen.

---

1. Auftragsverarbeitungsvertrag (= Data Processing Addendum, DPA) prüfen.

Der Auftragsverarbeitungsvertrag ist eine Anforderung des Art. 28 DSGVO, ohne den Sie keine Daten an Dritte übertragen dürfen.

Mit Abschluss des Vertrages ("Terms of Use") mit Hedy AI LLC schließen Sie auch einen Auftragsverarbeitungsvertrag ("**Data Processing Addendum**", DPA) mit Hedy AI LLC ab. Der DPA und die mitgeltenden **Anhänge I bis III** ("Annex") stehen im Trust Center zur Verfügung.

- **Ihre Aufgabe:** Prüfen Sie diese Dokumente und stellen Sie sicher, dass der Auftragsverarbeitungsvertrag mit seinen Anhängen aus Ihrer Sicht einen angemessenen Rahmen für die Verarbeitung sicherstellt..
- **Fragen Sie sich:**
    - Entsprechen die Inhalte den Anforderungen aus Art. 28 DSGVO und passen sie zu Ihrer beabsichtigten Verarbeitung?
    - Sind die Annexe zum Data Processing Addendum angemessen?
- **Dokumentation:** Dokumentieren Sie Ihre vorgenommenen Prüfungen und das Ergebnis Ihrer Bewertung. Legen Sie diese Dokumentation zusammen mit den geprüften Dokumenten als Kopie ab.

---

2. Drittlandtransfer (SCCs und TIA) prüfen und dokumentieren

Hedy AI LLC hat seinen Sitz in den USA. Daher werden zur Nutzung der Services Daten in ein Drittland (USA) übermittelt, sofern die Verarbeitung nicht ausschließlich auf Ihrem Endgerät stattfindet. Garantie für diesen Datentransfer an Hedy AI LLC sind die EU-Standardvertragsklauseln (SCCs). Die DSGVO (und die Rechtsprechung, "Schrems II") verlangt, dass Sie die Wirksamkeit dieser Klauseln bewerten.

Hedy AI LLC stellt Ihnen im Trust Center ein **Transfer Impact Assessment (TIA)** zur Verfügung, das die Rechtslage in den USA und die von Hedy AI LLC getroffenen zusätzlichen Maßnahmen bewertet.

- **Ihre Aufgabe:** Sie müssen die Schlussfolgerungen des TIA für Ihren spezifischen Anwendungsfall (Ihre Daten, Ihre Übermittlung, Ihre Einstellungen) nachvollziehen, prüfen und sich zu eigen machen.
- **Fragen Sie sich:**
    - Sind die SCCs über das Data Processing Addendum wirksam eingebunden?
    - Wird durch die TIA für mich nachvollziehbar, dass die übertragenen personenbezogenen Daten ein ausreichendes und mit der EU gleichwertiges Schutzniveau haben?
- **Dokumentation:** Dokumentieren Sie, dass die SCCs als Garantie für den Transfer wirksam sind, dass Sie das TIA geprüft haben und zu dem Schluss gekommen sind, dass für die von Ihnen übermittelten Daten ein angemessenes Schutzniveau (unter Einbeziehung der SCCs und der Maßnahmen im TIA) gewährleistet ist.

3. Technische und Organisatorische Maßnahmen (TOMs) bewerten

Hedy AI LLC stellt Ihnen im Trust Center als **Annex II** eine detaillierte Beschreibung seiner **Technischen und Organisatorischen Maßnahmen (TOMs)** gemäß Art. 32 DSGVO zur Verfügung.

- **Ihre Aufgabe:** Sie müssen prüfen und bewerten, ob diese Maßnahmen ein angemessenes Schutzniveau für die *beabsichtigte Verarbeitung* über Hedy AI LLC und die *spezifischen Datenkategorien* bieten.
- **Fragen Sie sich:**
    - Verarbeite ich nur Namen von Personen oder potenziell sensible Informationen gemäß Art. 9 DSGVO?
    - Habe ich erhöhte Pflichten zum Datenschutz, zur Geheimhaltung oder zur IT-Sicherheit?
    - Wird durch die TOMs für mich nachvollziehbar ein ausreichendes Schutzniveau für die Verarbeitung sichergestellt?
- **Dokumentation:** Dokumentieren Sie Ihre Überlegungen und das Ergebnis Ihrer Bewertung. Legen Sie diese Dokumentation zusammen mit dem TOM-Dokument ab.

---

4. Unterauftragsverarbeiter (= Sub-Processors) prüfen

Hedy AI LLC setzt für die Leistungserbringung teilweise Unterauftragsverarbeiter ein, z.B. für die Cloud-Speicherung oder KI-Dienste.

Hedy AI LLC stellt Ihnen im Trust Center als **Annex III** eine "**List of Sub-Processors**" zur Verfügung und hat sich im Data Processing Addendum verpflichtet, Sie über Änderungen der Unterauftragsverarbeiter vorab zu informieren.

- **Ihre Aufgabe:** Gemäß Art. 28 Abs. 2 DSGVO müssen Sie als Verantwortlicher die eingesetzten Sub-Prozessoren (initial) genehmigen. Stellen Sie auch sicher, dass Sie einen Prozess zur Bewertung bei *neuen* Sub-Prozessoren bei sich intern etabliert haben.
- **Fragen Sie sich:**
    - Ist die Liste der Sub-Prozessoren nachvollziehbar und transparent?

    - Für Sub-Prozessoren in einem Drittland: Wurde der Datentransfer im Rahmen des Transfer Impact Assessments (TIA) von Hedy AI LLC ausreichend bewertet und abgesichert?
    - Sind die im Auftragsverarbeitungsvertrag enthaltenen Formulierungen zu Sub-Prozessoren ausreichend, um gemäß Art. 28 Abs. 4 DSGVO die Pflichten aus der Auftragsverarbeitung von Hedy AI LLC auf die Unterauftragsverarbeiter zu übertragen?
    - Was ist mein interner Prozess, wenn Hedy einen neuen Sub-Prozessor ankündigt?
- **Dokumentation:** Dokumentieren Sie Ihre Prüfung und Genehmigung der aktuellen Sub-Prozessor-Liste (als Kopie). Halten Sie fest, dass die vertraglichen Grundlagen (insb. für Drittlandtransfers und die Pflichten nach Art. 28 Abs. 4) als ausreichend bewertet wurden. Dokumentieren Sie auch, wie Sie den Bewertungsprozess bei Änderungen sicherstellen und mit Einwänden umgehen wollen.

Aktualisierung

Die von Ihnen mit Hilfe dieser Checkliste hergestellte und dokumentierte DSGVO-Compliance ist eine Momentaufnahme. Wesentliche Änderungen können eine Neubewertung der Datenschutz-Konformität erforderlich machen. Dies sind insbesondere (aber nicht nur):

- Änderungen an Ihrer eigenen Verarbeitung (insbesondere Veränderung der verarbeiteten personenbezogenen Daten)
- Änderungen an Ihrem Verwendungszweck
- Erweiterung der Anwendungsfälle oder Einsatzgebiete
- Gesetzesänderungen oder neue Reschtsprechung
- Änderungen der Servicebereitstellung seitens Hedy AI LLC oder seiner Sub-Prozessoren

Sobald Sie von solchen Änderungen erfahren, sollten Sie umgehend prüfen, ob eine neue Datenschutz-Bewertung erforderlich ist.

Um die Datenschutz-Dokumentation als Nachweis aktuell zu halten, ist ein Review mindestens in jährlichem Abstand durchzuführen und zu dokumentieren - auch wenn es keine bekannten Änderungen gegeben hat.