Vertrag zur Auftragsverarbeitung

nach Art. 28 Abs. 3 DSGVO für den Dienst Hexlizer · Fassung vom 16. September 2026 · wortgleich mit hexlizer.de/avv.html

zwischen

Firma: ..... Anschrift: .....
vertreten durch: ..... – nachfolgend „Verantwortlicher" –

und

BlackHexagon UG (haftungsbeschränkt), Am Holderspfad 139, 47809 Krefeld, eingetragen im Handelsregister des Amtsgerichts Krefeld unter HRB 19706, vertreten durch den Geschäftsführer Norbert Hans Traut – nachfolgend „Auftragsverarbeiter" –

---

§ 1 Gegenstand und Dauer

1. Der Auftragsverarbeiter betreibt den Dienst Hexlizer, mit dem Endkunden des Verantwortlichen Fahrzeugfotos hochladen und Visualisierungen in Folien aus dem Katalog des Verantwortlichen erhalten. Dieser Vertrag regelt die dabei stattfindende Verarbeitung personenbezogener Daten im Auftrag.
2. Hauptvertrag ist der Nutzungsvertrag nach § 3 Abs. 1 der AGB; die Dauer dieses Vertrags entspricht dessen Laufzeit. Der Vertrag endet mit dem Hauptvertrag; die Pflichten zur Löschung gelten darüber hinaus.

§ 2 Art, Zweck, Datenkategorien, Betroffene

Merkmal	Festlegung
Art der Verarbeitung	Empfang, Speicherung, Verkleinerung, Entfernen von Metadaten, Übermittlung an den Unterauftragsverarbeiter zum Rendern, Speicherung und Bereitstellung des Ergebnisbildes, Löschung
Zweck	Erzeugung einer Visualisierung des Fahrzeugs des Endkunden in einer gewählten Folie; auf Wunsch des Endkunden öffentliche Bereitstellung des Ergebnisses (Teilen)
Datenkategorien	Fahrzeugfotos (ggf. mit Kennzeichen, Personen, Umgebung), erzeugte Ergebnisbilder, gewählte Folie, Zeitstempel, gehashte und gekürzte IP-Adresse, Auftrags-Token, technische Browserdaten, aus dem Foto erkannte Fahrzeugmerkmale (Marke, Modell, Karosserieform, ungefähres Baujahr, geschätzte Maße); bei freiwilliger Anmeldung des Endkunden zusätzlich E-Mail-Adresse, Anzeigename, optional Telefonnummer und Bildstand
Betroffene	Endkunden und Website-Besucher des Verantwortlichen; ggf. auf Fotos abgebildete Dritte
Besondere Kategorien	Nicht vorgesehen und nicht Gegenstand des Auftrags. Der Verantwortliche weist seine Endkunden an, möglichst Fotos ohne erkennbare Personen zu verwenden und Fotos mit erkennbaren Personen nur mit deren Einwilligung hochzuladen. Der Dienst erkennt Personen und verwendet solche Bilder für freigegebene Zwecke ausschließlich unkenntlich gemacht

§ 3 Weisungen

1. Der Auftragsverarbeiter verarbeitet Daten nur auf dokumentierte Weisung des Verantwortlichen. Die Weisungen sind durch diesen Vertrag, die AGB und die Konfiguration des Mandanten (Katalog, Domains, Limits, Badge) festgelegt. Weitere Weisungen erteilt der Verantwortliche in Textform.
2. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich und darf die Ausführung bis zur Klärung aussetzen.

§ 4 Pflichten des Auftragsverarbeiters

1. Er verpflichtet die zur Verarbeitung befugten Personen zur Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO).
2. Er trifft die technischen und organisatorischen Maßnahmen nach § 7 (Art. 32 DSGVO).
3. Er unterstützt den Verantwortlichen bei der Beantwortung von Betroffenenanfragen (Art. 12–22 DSGVO), soweit ihm das möglich ist; Anfragen, die direkt beim Auftragsverarbeiter eingehen, leitet er unverzüglich weiter.
4. Er unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung) unter Berücksichtigung der Art der Verarbeitung.
5. Er meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis. Die Erstmeldung erfolgt auch

dann, wenn noch nicht alle Angaben nach Art. 33 Abs. 3 DSGVO vorliegen; fehlende Angaben reicht der Auftragsverarbeiter unverzüglich nach.

6. Er stellt alle Informationen zum Nachweis der Einhaltung dieses Vertrags zur Verfügung und ermöglicht Überprüfungen nach § 8.
7. Ein Datenschutzbeauftragter ist beim Auftragsverarbeiter derzeit nicht bestellt. Die Schwellenregelung des § 38 Abs. 1 Satz 1 BDSG greift nicht; die weiteren Fälle desselben Absatzes sowie Art. 37 DSGVO werden geprüft. Der Auftragsverarbeiter benennt eine Ansprechperson für Datenschutzfragen und teilt dem Verantwortlichen unverzüglich mit, falls eine Benennungspflicht entsteht.

---

§ 5 Unterauftragsverarbeiter

1. Der Verantwortliche genehmigt allgemein den Einsatz der folgenden Unterauftragsverarbeiter:

Unternehmen	Leistung	Ort	Übermittlungsgrundlage
OpenAI Ireland Limited, Dublin, Irland (Vertragspartner für den Europäischen Wirtschaftsraum)	Erzeugung des Ergebnisbildes und Erkennung des Fahrzeugs; Eingabe: Fahrzeugfoto und Farbmuster	Verarbeitung auf Servern in den USA; EU-Datenresidenz derzeit nicht aktiviert	EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914) als Bestandteil des OpenAI Data Processing Addendum; keine Nutzung der Inhalte zum Modelltraining nach den Bedingungen der Schnittstelle; Protokolle zur Missbrauchserkennung nach Angaben von OpenAI regelmäßig bis zu 30 Tage, in Ausnahmefällen länger, wenn OpenAI gesetzlich dazu verpflichtet ist oder es zur Untersuchung von Missbrauch erforderlich ist. Unterauftragnehmer von OpenAI: platform.openai.com/subprocessors
TipTopCarbon GmbH, Im Lindental 48, 58135 Hagen, Deutschland	Stellt derzeit den Zugang zur OpenAI-Schnittstelle bereit, über den die Bilder verarbeitet werden	Deutschland; die Verarbeitung selbst findet bei OpenAI statt	Vereinbarung zur Unterauftragsverarbeitung zwischen Auftragsverarbeiter und TipTopCarbon GmbH (Fassung vom 11. September 2026); die Mitnutzung des Zugangs ist nach der OpenAI-Dienstvereinbarung für verbundene Unternehmen vorgesehen. Diese Stufe entfällt, sobald die BlackHexagon UG (haftungsbeschränkt) einen eigenen Zugang nutzt
ALL-INKL.COM – Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf, Deutschland	Hosting des Dienstes, Speicherung von Fotos, Ergebnissen und Datenbank	Deutschland	Verarbeitung innerhalb der EU; Auftragsverarbeitungsvertrag mit dem Hoster
Google Ireland Limited, Dublin, Irland – **derzeit nicht in Betrieb**	Anmeldung eines Endkunden mit Google-Konto. Die Funktion ist vorbereitet, aber nicht aktiviert; es werden keine Daten an Google übermittelt	–	Vor einer Aktivierung werden Rolle und Rechtsgrundlage bestimmt und der Verantwortliche nach § 5 Abs. 2 vorab informiert

2. Beabsichtigte Änderungen (Hinzufügen oder Ersetzen) teilt der Auftragsverarbeiter dem Verantwortlichen mindestens 4 Wochen vorher in Textform mit. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen; kommt keine Einigung zustande, darf er den Hauptvertrag außerordentlich kündigen und erhält nicht verbrauchtes Guthaben anteilig erstattet.

3. Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter vertraglich auf ein Datenschutzniveau, das diesem Vertrag entspricht, und bleibt gegenüber dem Verantwortlichen für deren Pflichterfüllung verantwortlich.

---

§ 6 Löschung und Rückgabe

1. Ein stündlich laufender Löschlauf entfernt hochgeladene Fotos und Ergebnisbilder, deren Upload mehr als 23 Stunden zurückliegt; maßgeblich ist der Zeitpunkt des Hochladens, nicht der Zeitpunkt der Bilderzeugung. Im Regelfall ist ein Bild damit spätestens 24 Stunden nach dem Hochladen gelöscht. Der Auftragsverarbeiter überwacht das Alter des ältesten gespeicherten Bildes und wird bei Überschreitung benachrichtigt; bei einer Störung räumt er unverzüglich nach und unterrichtet den Verantwortlichen, wenn die Frist erheblich überschritten wurde. Ausgenommen sind geteilte Bilder nach Abs. 2 und Bilder mit einer Einwilligung nach Abs. 7.
2. Vom Endkunden ausdrücklich geteilte Ergebnisbilder werden **90 Tage** nach dem Teilen gelöscht; der Endkunde kann sie über einen Löschlink vorher entfernen. Der Verantwortliche kann die Löschung eines geteilten Bildes jederzeit anweisen.
3. Auftragsdaten ohne Bild (Zeitpunkt, Folie, Kosten, gehashte IP, erkanntes Fahrzeug) werden nach 90 Tagen gelöscht. Für die Abrechnung genügt die Zählung je Monat und Mandant; einzelne Auftragszeilen werden dafür nicht aufbewahrt.
4. Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter die noch vorhandenen Auftragsdaten binnen 30 Tagen oder gibt sie zurück; die Wahl zwischen Rückgabe und Löschung trifft der Verantwortliche. Er bestätigt die Löschung auf Verlangen. Kürzere Fristen aus Abs. 1 bis 3 bleiben unberührt und werden durch das Vertragsende nicht verlängert; bereits gelöschte Daten werden nicht erneut vorgehalten.
5. **Sicherungen und Wiederherstellung:** Die Löschpflichten dieses Paragrafen betreffen das aktive System. In Sicherungen des Hosting-Anbieters können gelöschte Daten enthalten bleiben, bis die jeweilige Sicherung nach dessen Zyklus entfernt wird; nach seiner Auskunft für dieses Paket sind das derzeit höchstens vier Wochen. Sicherungen werden ausschließlich zur Wiederherstellung nach einem Ausfall verwendet. Vor jeder Ausgabe geteilter oder archivierter Bilder und bevor eine Anmeldung am Endkundenkonto gilt, auch eine bestehende, fragt der Dienst ein Wachprogramm auf einem zweiten Server. Dieses kennt die höchste Zahl festgehaltener Löschungen und Widerrufe sowie die höchste Auftragsnummer; meldet der Dienst weniger, sperrt es die Ausgabe, unabhängig vom Alter der Sicherung. Die Sperre liegt auf dem zweiten Server, übersteht das Zurückspielen und wird nur durch eine ausdrückliche Freigabe aufgehoben, nachdem der Auftragsverarbeiter zwischenzeitliche Löschungen und Widerrufe erneut angewendet hat. Vor einer geplanten Wiederherstellung sperrt er vorher. Festgehalten werden entfernte öffentliche Links, gelöschte Archivbilder, zurückgenommene Einzelzwecke, auf Wunsch gelöschte Konten und von Hand vorgenommene Löschungen, etwa nach einem Widerspruch gegen die Auswertung; jeder Vorgang wird zusätzlich außerhalb des Dienstes und des Hosting-Pakets nachgewiesen. Antwortet das Wachprogramm nicht, gibt der Dienst sofort nichts mehr heraus. Kann eine Löschung dem Wachprogramm nicht gemeldet werden, wird sie trotzdem ausgeführt, der Auftragsverarbeiter gesondert gewarnt und die Meldung nachgeholt; hatte das Wachprogramm länger als drei Stunden keinen Kontakt zum Dienst, sperrt es von sich aus bis zum Abgleich. Vor jedem Einspielen einer

Sicherung und unmittelbar nach einer vom Hosting-Anbieter veranlassten Wiederherstellung prüft der Auftragsverarbeiter, ob eine solche Warnung offen ist.

6. Eine Rückgabe von Endkunden-Fotos ist im laufenden Betrieb nicht vorgesehen, da der Verantwortliche selbst keine Kopie erhält.
7. Erteilt ein Endkunde im Visualizer freiwillig eine gesonderte Einwilligung, dürfen die betroffenen Bilder über die Frist aus Abs. 1 hinaus gespeichert werden. Für die Zwecke „Verbesserung des Visualizers" und „Werbung für Hexlizer" ist die BlackHexagon UG (haftungsbeschränkt) eigene Verantwortliche; diese Verwendung geschieht außerhalb dieses Vertrags. Für den Zweck „Beispielbild im Shop" entscheidet der Verantwortliche über die Nutzung; die Bereitstellung an ihn erfolgt im Rahmen dieses Vertrags. Die Speicherung endet mit dem Widerruf, spätestens 3 Jahre nach der Freigabe. Widerrufe, die den Verantwortlichen betreffen, leitet der Auftragsverarbeiter unverzüglich weiter. Sind Personen erkennbar, wird ausschließlich eine unkenntlich gemachte Fassung bereitgestellt.

---

§ 7 Technische und organisatorische Maßnahmen (Kurzfassung)

- **Transportverschlüsselung:** Alle Verbindungen (Browser, Plugin, Unterauftragsverarbeiter) ausschließlich über TLS/HTTPS.
- **Datensparsamkeit:** Verkleinerung des Fotos bereits im Browser; Entfernen aller Metadaten (EXIF, Standort) beim Empfang; IP-Adressen nur gehasht und gekürzt.
- **Zugriffskontrolle:** Fotos und Ergebnisse sind nur über einen zufälligen, nicht erratbaren Token abrufbar; Speicherverzeichnisse sind für den Webzugriff gesperrt. Der Verwaltungsbereich ist mit einem langen, zufällig erzeugten Passwort geschützt, sperrt sich nach mehreren Fehlversuchen und verlangt zusätzlich einen zeitbasierten Einmalcode (Zwei-Faktor-Anmeldung, seit 10. September 2026 eingerichtet).
- **Mandantentrennung:** Katalog, Guthaben, Schlüssel und Statistiken sind je Mandant getrennt; öffentliche Schlüssel sind an die freigegebenen Domains gebunden.
- **Missbrauchsschutz:** Nutzungsgrenzen je Anschluss (Tag und 30 Tage), Guthaben-Obergrenzen, Kill-Switch je Mandant, Prüfung von Dateityp und Größe.
- **Löschkonzept:** Stündlicher automatischer Löschlauf; Bilder 23 Stunden ab dem Hochladen, geteilte Bilder 90 Tage, Auftragsdaten 90 Tage, längere Fristen nach § 6. Der Zustand ist über eine geschützte Statusadresse jederzeit prüfbar.
- **Verfügbarkeit und Sicherungen:** Die Datenbank liegt als Datei im Webspace. Nach Auskunft des Hosting-Anbieters für dieses Paket werden Datenbanken und Postfächer in der Regel alle 2–3 Tage und die Webspace-Daten etwa alle 14 Tage gesichert; die Sicherungen werden derzeit höchstens 4 Wochen vorgehalten. Erfasst werden webseitenrelevante Dateien, also auch Datenbank und Bildordner. Der Anbieter bezeichnet die Sicherung ausdrücklich als freiwillige Leistung ohne Anspruch; eine verbindliche Zusage über Zahl und Höchstalter der Sicherungen ist damit nicht verbunden. Eigene zusätzliche Sicherungen der Auftragsdaten legt der Auftragsverarbeiter nicht an. Sicherungen werden ausschließlich zur Wiederherstellung nach einem Ausfall verwendet.
- **Organisation:** Verpflichtung der Mitarbeitenden auf Vertraulichkeit; dokumentierte Unterauftragsverarbeiter; jährliche Überprüfung der Maßnahmen.

§ 8 Kontrollrechte

1. Der Verantwortliche kann die Einhaltung dieses Vertrags jederzeit durch Einholung von Auskünften und Vorlage von Nachweisen überprüfen (z. B. Beschreibung der Maßnahmen, Nachweise der Unterauftragsverarbeiter). Darüber hinaus kann er einmal jährlich sowie bei einem konkreten Anlass, insbesondere nach einer Verletzung des Schutzes personenbezogener Daten, nach Ankündigung mit angemessener Frist während der Geschäftszeiten vor Ort prüfen oder prüfen lassen.
2. Für Prüfungen, die über die jährliche Prüfung und anlassbezogene Prüfungen hinausgehen, darf der Auftragsverarbeiter einen angemessenen Aufwandsersatz verlangen. Für anlassbezogene Prüfungen nach einer von ihm zu vertretenden Verletzung trägt er die eigenen Kosten.

§ 9 Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung verantwortlich. Er stellt insbesondere sicher, dass für die Verarbeitung der Endkundenfotos eine tragfähige Rechtsgrundlage besteht, dass die Information nach Art. 13 DSGVO (einschließlich der Übermittlung an OpenAI und der Speicherdauern) vor dem Hochladen erfolgt und dass die Nutzungshinweise nach § 7 der AGB angezeigt werden. Welche Rechtsgrundlage er wählt und wie er sie dokumentiert, bestimmt er selbst; der Auftragsverarbeiter stellt Mustertexte bereit.
2. Er informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 10 Haftung, Schlussbestimmungen

1. Für die Haftung gilt Art. 82 DSGVO; im Verhältnis der Parteien gilt ergänzend § 9 der AGB.
2. Änderungen und Ergänzungen bedürfen der Textform. Bei Widersprüchen zwischen diesem Vertrag und den AGB geht dieser Vertrag in datenschutzrechtlichen Fragen vor.
3. Es gilt deutsches Recht. Gerichtsstand ist Krefeld, sofern der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist; im Übrigen gelten die gesetzlichen Regeln.

Hauptvertrag

Grundlage ist der Hauptvertrag über die Nutzung des Dienstes Hexlizer nach den Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters und dem gewählten Paket.

Unterschriften

Verantwortlicher	Auftragsverarbeiter
Firma:	BlackHexagon UG (haftungsbeschränkt)
Ort, Datum:	Ort, Datum: .....
Unterschrift:	Unterschrift: .....
Name, Funktion:	Norbert Hans Traut, Geschäftsführer

Der Vertrag kann auf Papier oder elektronisch geschlossen werden (Art. 28 Abs. 9 DSGVO), im Kundenbereich durch Bestätigung des Händlers und Bestätigung des Auftragsverarbeiters per E-Mail.