

Auftragsverarbeitungsvertrag (AVV)

nach Art. 28 der Datenschutz-Grundverordnung (DSGVO)

Version 1.0 · Stand: Oktober 2026

Geltung

Dieser Auftragsverarbeitungsvertrag („AVV“) gilt zwischen der

nebty GmbH, c/o BASE Coworking, Blütenstraße 15, 80799 München, eingetragen im Handelsregister des Amtsgerichts München unter HRB 293827 („nebty“),

und dem Unternehmen, das Leistungen von nebty auf Grundlage der Allgemeinen Geschäftsbedingungen von nebty oder eines individuell geschlossenen Vertrags bezieht (der „Kunde“; der jeweilige Vertrag über die Leistungen der „Hauptvertrag“).

Der AVV wird mit Abschluss des Hauptvertrags – durch Abschluss des Bestellprozesses, Freischaltung des Kundenkontos oder Unterzeichnung – Bestandteil des Hauptvertrags. Einer gesonderten Unterzeichnung bedarf es nicht; das elektronische Format genügt der Form nach Art. 28 Abs. 9 DSGVO. Auf Anfrage stellt nebty eine gegengezeichnete Fassung zur Verfügung.

§ 1 Gegenstand, Anwendungsbereich und Dauer

(1) nebty erbringt für den Kunden Leistungen im Bereich Brand Protection, insbesondere die Überwachung von Online-Kanälen auf Markenmissbrauch („Monitoring“), die Durchsetzung der Entfernung rechtsverletzender Inhalte („Takedown“), die Bereitstellung der nebty-Plattform sowie den Zugang über Programmierschnittstellen (zusammen die „Leistungen“). Soweit nebty dabei personenbezogene Daten im Auftrag des Kunden verarbeitet, gilt dieser AVV.

(2) Der kostenlose Website-Scanner und sonstige Angebote, die ohne Kundenkonto genutzt werden, sind nicht Gegenstand dieses AVV.

(3) Die Laufzeit dieses AVV entspricht der Laufzeit des Hauptvertrags. Pflichten, die ihrer Natur nach über das Vertragsende hinaus fortbestehen, insbesondere nach §§ 5 Abs. 1 und 12, gelten fort, solange nebty personenbezogene Daten des Kunden verarbeitet.

§ 2 Art und Zweck der Verarbeitung, Datenarten und betroffene Personen

(1) Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

(2) Der Kunde ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. nebty ist Auftragsverarbeiterin.

(3) Verarbeitet der Kunde die Daten seinerseits im Auftrag eines Dritten – etwa als Managed Service Provider, Agentur oder Reseller für die Marken seiner Endkunden –, ist nebty weitere Auftragsverarbeiterin. Der Kunde stellt sicher, dass seine Weisungen von denen seines Verantwortlichen gedeckt sind und dass dieser AVV die Anforderungen des Art. 28 Abs. 4 DSGVO in seinem Verhältnis zum Verantwortlichen erfüllt. Rechte des Verantwortlichen gegenüber nebty übt der Kunde aus.

§ 3 Verarbeitung in eigener Verantwortung von nebty

(1) Nicht Gegenstand dieses AVV sind Verarbeitungen, für die nebty selbst Verantwortliche ist. Das sind insbesondere:

1. die Vertragsverwaltung, Abrechnung und Zahlungsabwicklung sowie die Kommunikation mit dem Kunden über das Vertragsverhältnis,
2. die Gewährleistung der Sicherheit und Stabilität der eigenen Systeme, einschließlich der Abwehr missbräuchlicher Zugriffe,
3. die Aufbewahrung von Unterlagen, die dem Nachweis der ordnungsgemäßen Leistungserbringung dienen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind, sowie die Erfüllung gesetzlicher Aufbewahrungspflichten.

(2) nebty darf technische Bedrohungsindikatoren, die bei der Leistungserbringung anfallen – insbesondere Domainnamen, URLs, IP-Adressen, Hashwerte sowie Angaben zu Hosting-Anbietern und Registraren betrügerischer Angebote –, sowie anonymisierte oder aggregierte Auswertungen nutzen, um ihre Erkennungsverfahren zu verbessern und andere Kunden vor denselben Angriffen zu schützen. Die Identität des Kunden, seine Marken und Fallakten werden dabei nicht offengelegt. Soweit solche Indikatoren ausnahmsweise einen Personenbezug aufweisen, verarbeitet nebty sie in eigener Verantwortung auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO.

(3) Stellen, an die nebty im Rahmen des Takedowns Meldungen richtet – etwa Registrare, Hosting-Anbieter, Plattformbetreiber, Suchmaschinen und Betreiber von Sicherheits-Blacklists –, verarbeiten die übermittelten Daten in eigener Verantwortung. Sie sind keine Unterauftragsverarbeiter im Sinne dieses AVV.

§ 4 Weisungen

(1) nebty verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden, auch in Bezug auf die Übermittlung in Drittländer, es sei denn, nebty ist durch das Recht der Union oder eines Mitgliedsstaats zur Verarbeitung verpflichtet. In diesem Fall teilt nebty dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Hauptvertrag, dieser AVV und die vom Kunden in der Plattform oder über die Programmierschnittstellen vorgenommenen Einstellungen und Aufträge – etwa die Anlage einer Marke, die Auswahl der überwachten Kanäle oder die Beauftragung eines Takedowns – bilden die Weisungen des Kunden. Weitere Weisungen erteilt der Kunde in Textform (E-Mail genügt).

(3) nebty informiert den Kunden unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt. nebty darf die Ausführung der Weisung aussetzen, bis der Kunde sie bestätigt oder ändert.

(4) Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, behandeln die Parteien als Antrag auf Leistungsänderung.

§ 5 Pflichten von nebty

(1) **Vertraulichkeit.** nebty gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und nur insoweit Zugriff auf die Daten erhalten, wie es für die Leistungserbringung erforderlich ist.

(2) **Sicherheit der Verarbeitung.** nebty trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die Maßnahmen zum Zeitpunkt des Vertragsschlusses beschreibt **Anlage 2**. nebty darf die Maßnahmen dem technischen Fortschritt anpassen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert nebty.

(3) **Zweckbindung.** nebty verarbeitet die Daten des Kunden nur zur Erbringung der Leistungen und vorbehaltlich § 3 zu keinem anderen Zweck. nebty verkauft die Daten nicht und nutzt sie nicht zum Training von KI-Modellen Dritter; nebty setzt KI-Dienste nur unter Bedingungen ein, die eine Nutzung der übermittelten Daten zum Modelltraining durch den Anbieter ausschließen.

(4) **Verarbeitungsort.** Die nebty-Plattform einschließlich Datenbank und der Ablage von Beweismitteln wird in Rechenzentren in Deutschland betrieben. Einzelne Unterauftragsverarbeiter verarbeiten Daten außerhalb des Europäischen Wirtschaftsraums; es gilt § 7.

(5) **Verzeichnis.** nebty führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten, die sie im Auftrag ihrer Kunden durchführt (Art. 30 Abs. 2 DSGVO).

(6) **Ansprechpartner.** Ansprechpartner für Fragen des Datenschutzes bei nebty ist erreichbar unter info@nebty-id.com.

§ 6 Unterauftragsverarbeiter

(1) Der Kunde erteilt nebty die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in der Liste nach **Anlage 3** aufgeführt und gelten als genehmigt.

(2) nebty informiert den Kunden mindestens **dreißig (30) Tage** vor der Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Die Information erfolgt durch Aktualisierung der Liste nach Anlage 3 und durch Mitteilung per E-Mail an die im Kundenkonto hinterlegte Adresse des Kontoinhabers sowie an Kunden, die sich für Änderungsmitteilungen registriert haben.

(3) Der Kunde kann der Änderung innerhalb von vierzehn (14) Tagen nach Zugang der Mitteilung aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Die Parteien bemühen sich dann um eine einvernehmliche Lösung. Kommt diese nicht innerhalb angemessener Frist zustande, kann jede Partei die von der Änderung betroffenen Leistungen mit Wirkung zum Zeitpunkt des Wirksamwerdens der Änderung kündigen. Für den nicht genutzten Zeitraum im Voraus gezahlte Entgelte erstattet nebty zeitanteilig.

(4) Ist der Austausch eines Unterauftragsverarbeiters kurzfristig erforderlich, um die Sicherheit oder Verfügbarkeit der Leistungen zu gewährleisten, darf nebty ihn ohne Einhaltung der Frist nach Absatz 2 vornehmen. nebty informiert den Kunden in diesem Fall unverzüglich; das Widerspruchsrecht nach Absatz 3 bleibt unberührt.

(5) nebty erlegt jedem Unterauftragsverarbeiter vertraglich im Wesentlichen dieselben Datenschutzpflichten auf, die in diesem AVV festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. nebty haftet gegenüber dem Kunden für die Einhaltung dieser Pflichten durch den Unterauftragsverarbeiter.

(6) Nicht als Unterauftragsverarbeitung gelten Nebenleistungen, die nebty bei Dritten in Anspruch nimmt, ohne dass diese bestimmungsgemäß Zugriff auf personenbezogene Daten des Kunden erhalten, etwa Telekommunikationsleistungen oder die Bereitstellung von Software zum Betrieb in eigener Umgebung.

§ 7 Übermittlungen in Drittländer

(1) Eine Übermittlung personenbezogener Daten in ein Land außerhalb des Europäischen Wirtschaftsraums erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Für Übermittlungen an Unterauftragsverarbeiter stützt sich nebty auf einen Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO – für Empfänger in den Vereinigten Staaten auf eine aktive Zertifizierung nach dem EU-U.S. Data Privacy Framework – oder auf die Standardvertragsklauseln der Europäischen Kommission nach dem Durchführungsbeschluss (EU) 2021/914 (Art. 46 Abs. 2 lit. c DSGVO). Die jeweilige Grundlage ist in Anlage 3 angegeben. Entfällt eine Grundlage, stellt nebty die Übermittlung auf eine andere zulässige Grundlage um oder setzt sie aus.

(3) Erfolgt eine Übermittlung vom Kunden an nebty aus einem Drittland oder greift der Kunde aus einem Drittland auf die Plattform zu, gelten, soweit erforderlich, die Standardvertragsklauseln (Modul 2, bei Kunden nach § 2 Abs. 3 Modul 3) als zwischen den Parteien vereinbart. Dabei gilt: Klausel 7 ist nicht anwendbar; für Klausel 9 gilt Option 2 mit der Frist nach § 6 Abs. 2; die fakultative Regelung in Klausel 11 ist nicht anwendbar; für Klausel 17 und 18 gelten das Recht der Bundesrepublik Deutschland und die Gerichte in München. Die Anhänge der Standardvertragsklauseln werden durch die Anlagen 1 bis 3 ausgefüllt; zuständige Aufsichtsbehörde ist das Bayerische Landesamt für Datenschutzaufsicht. Für Übermittlungen, die dem Datenschutzrecht des Vereinigten Königreichs oder der Schweiz unterliegen, gelten die Standardvertragsklauseln mit den dafür vorgesehenen Anpassungen (UK International Data Transfer Addendum bzw. Anpassungen nach Vorgabe des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten).

(4) **Meldungen im Rahmen des Takedowns.** Ein Takedown erfordert, dass nebty dem für einen beanstandeten Inhalt zuständigen Anbieter eine Meldung samt Beweismitteln übermittelt; diese Anbieter können ihren Sitz weltweit haben. Mit der Beauftragung eines Takedowns weist der Kunde nebty an, diese Meldungen zu übermitteln. nebty prüft vor jeder Meldung an einen Empfänger außerhalb des Europäischen Wirtschaftsraums, ob ein Angemessenheitsbeschluss oder geeignete Garantien bestehen. Ist das nicht der Fall, stützt sich die Übermittlung auf Art. 49 Abs. 1 lit. e DSGVO, soweit sie zur Geltendmachung der Rechte des Kunden gegenüber dem jeweiligen Anbieter erforderlich ist. nebty begrenzt den Inhalt jeder Meldung auf das für den jeweiligen Empfänger Erforderliche und schwärzt personenbezogene Bestandteile, die für die Bearbeitung nicht benötigt werden.

§ 8 Unterstützung des Kunden

(1) nebty unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III der DSGVO zu beantworten. Richtet eine betroffene Person einen Antrag unmittelbar an nebty, leitet nebty ihn unverzüglich an den Kunden weiter und beantwortet ihn nicht ohne Weisung des Kunden, sofern die Zuordnung zum Kunden möglich ist.

(2) nebty unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der Aufsichtsbehörde.

(3) Unterstützungsleistungen nach diesem § 8, die über die in der Plattform bereitgestellten Funktionen hinausgehen und nicht durch einen Verstoß von nebty veranlasst sind, kann nebty dem Kunden nach vorheriger Ankündigung zu angemessenen Sätzen in Rechnung stellen.

§ 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) nebty meldet dem Kunden jede Verletzung des Schutzes personenbezogener Daten, die Daten des Kunden betrifft, unverzüglich, spätestens innerhalb von **achtundvierzig (48) Stunden** nach Bekanntwerden.

(2) Die Meldung enthält, soweit bekannt, eine Beschreibung der Art der Verletzung einschließlich der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen, die ergriffenen oder vorgeschlagenen Maßnahmen sowie einen Ansprechpartner. Informationen, die noch nicht vorliegen, reicht nebty unverzüglich nach.

(3) nebty ergreift unverzüglich die erforderlichen Maßnahmen zur Eindämmung der Verletzung und zur Minderung ihrer Folgen und unterstützt den Kunden bei der Erfüllung seiner Melde- und Benachrichtigungspflichten. Meldungen an Aufsichtsbehörden oder betroffene Personen nimmt nebty im Namen des Kunden nur auf dessen Weisung vor.

§ 10 Nachweise und Kontrollen

(1) nebty stellt dem Kunden auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO und diesem AVV zur Verfügung, insbesondere die jeweils aktuelle Beschreibung der technischen und organisatorischen Maßnahmen und die Vertragsgrundlagen der Unterauftragsverarbeiter. Geeignete Zertifizierungen oder Prüfberichte unabhängiger Stellen können als Nachweis dienen.

(2) Der Kunde kann darüber hinaus Überprüfungen einschließlich Inspektionen durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen, der kein Wettbewerber von nebty ist. Überprüfungen finden nach Ankündigung mit einer Frist von mindestens dreißig (30) Tagen, in der Regel höchstens einmal je Kalenderjahr, während der üblichen Geschäftszeiten und ohne unverhältnismäßige Störung des Betriebs statt. Anlassbezogene Überprüfungen nach einer Verletzung des Schutzes personenbezogener Daten sowie Überprüfungen auf Verlangen einer Aufsichtsbehörde sind hiervon ausgenommen.

(3) Die Kosten einer Überprüfung trägt der Kunde. Für den eigenen Aufwand kann nebty eine angemessene Vergütung verlangen, es sei denn, die Überprüfung deckt einen wesentlichen Verstoß von nebty gegen diesen AVV auf.

(4) Prüfungsrechte gelten nicht für Informationen, die Geschäftsgeheimnisse von nebty oder Daten anderer Kunden betreffen, sowie für Systeme von Unterauftragsverarbeitern; insoweit stellt nebty die von diesen erhaltenen Nachweise zur Verfügung, soweit sie zur Weitergabe berechtigt ist.

§ 11 Pflichten des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für das Vorliegen einer Rechtsgrundlage und die Erfüllung der Informationspflichten gegenüber den betroffenen Personen. Dies gilt auch für die Auswahl der zu überwachenden Marken, Kennzeichen und Suchbegriffe und für die Beauftragung von Takedowns.

(2) Der Kunde stellt nebty keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO und keine Daten im Sinne des Art. 10 DSGVO zur Verarbeitung bereit, es sei denn, dies ist zur Leistungserbringung unvermeidbar und vorab vereinbart. Dass beanstandete fremde Inhalte im Einzelfall solche Daten enthalten, bleibt unberührt.

(3) Der Kunde informiert nebty unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

(4) Der Kunde ist für die Verwaltung der Nutzerkonten seiner Organisation verantwortlich, insbesondere für die Vergabe und den Entzug von Zugängen und den Schutz der Zugangsdaten. Leitet der Kunde Benachrichtigungen an eigene Systeme oder Dienste Dritter weiter – etwa per Webhook, an Messenger-Kanäle oder über Programmierschnittstellen an eigene Anwendungen –, liegt die Verarbeitung ab Übergabe in seiner Verantwortung.

§ 12 Löschung und Rückgabe

(1) Der Kunde kann seine Daten während der Laufzeit des Hauptvertrags über die Plattform und die Programmierschnittstellen exportieren. Auf Anforderung stellt nebty die Daten innerhalb von zehn (10) Werktagen nach Vertragsende in einem gängigen, maschinenlesbaren Format bereit.

(2) Nach Beendigung des Hauptvertrags löscht nebty die im Auftrag verarbeiteten personenbezogenen Daten innerhalb von dreißig (30) Tagen, sofern der Kunde nicht zuvor die Rückgabe verlangt hat. Kopien in Datensicherungen werden im Rahmen der regulären Sicherungszyklen überschrieben, spätestens nach neunzig (90) Tagen. Bis dahin unterliegen sie den Pflichten dieses AVV und werden nicht aktiv verarbeitet.

(3) Absatz 2 gilt nicht, soweit nach dem Recht der Union oder eines Mitgliedstaats eine Pflicht zur Speicherung besteht, sowie für Daten nach § 3 Abs. 1 Nr. 3. Die Löschung bestätigt nebty auf Verlangen in Textform.

§ 13 Haftung

- (1) Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO.
- (2) Im Verhältnis der Parteien gelten die Haftungsregelungen des Hauptvertrags, soweit nicht zwingendes Recht oder die Standardvertragsklauseln entgegenstehen.

§ 14 Regulierte Kunden

Ist der Kunde ein Finanzunternehmen im Sinne der Verordnung (EU) 2022/2554 (DORA) oder unterliegt er vergleichbaren aufsichtsrechtlichen Anforderungen an die Auslagerung, vereinbaren die Parteien auf Anfrage eine ergänzende Vereinbarung, insbesondere zu den Anforderungen des Art. 30 DORA. neby stellt hierfür ein Muster bereit.

§ 15 Schlussbestimmungen

- (1) **Rangfolge.** Bei Widersprüchen gelten in folgender Reihenfolge: (a) die Standardvertragsklauseln, soweit sie nach § 7 anwendbar sind; (b) ein zwischen den Parteien individuell unterzeichneter Auftragsverarbeitungsvertrag; (c) dieser AVV; (d) der Hauptvertrag. Dieser AVV geht dem Hauptvertrag in allen Fragen der Verarbeitung personenbezogener Daten vor.
- (2) **Änderungen.** neby kann diesen AVV ändern, soweit dies zur Anpassung an geänderte rechtliche Anforderungen oder an Änderungen der Leistungen erforderlich ist und das Schutzniveau für den Kunden nicht sinkt. neby teilt Änderungen mindestens sechs (6) Wochen vor ihrem Wirksamwerden in Textform mit. Widerspricht der Kunde nicht innerhalb dieser Frist, gilt die Änderung als genehmigt; auf diese Folge weist neby in der Mitteilung hin. Widerspricht der Kunde, gilt der AVV in der bisherigen Fassung fort; das Recht beider Parteien zur ordentlichen Kündigung des Hauptvertrags bleibt unberührt. Änderungen der Liste der Unterauftragsverarbeiter richten sich allein nach § 6.
- (3) **Recht und Gerichtsstand.** Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist München, soweit der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.
- (4) **Salvatorische Klausel.** Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.
- (5) **Sprache.** Maßgeblich ist die deutsche Fassung dieses AVV. Die englische Fassung dient der Information.
-

Anlage 1 – Beschreibung der Verarbeitung

Gegenstand und Dauer: Erbringung der Leistungen nach dem Hauptvertrag für dessen Laufzeit und bis zur Löschung nach § 12.

Häufigkeit: fortlaufend, soweit zur Erbringung der Leistungen erforderlich.

Leistung	Art und Zweck der Verarbeitung	Arten personenbezogener Daten	Betroffene Personen
Plattform und Kundenkonto	Bereitstellung der Plattform, Verwaltung von Nutzerkonten und Berechtigungen, Anmeldung, Benachrichtigungen per E-Mail und an vom Kunden eingerichtete Kanäle, Support	Name, dienstliche E-Mail-Adresse, Rolle und Berechtigungen, Anmelde- und Nutzungsdaten, IP-Adressen, Einstellungen, Support-Kommunikation	Beschäftigte und Beauftragte des Kunden; bei Kunden nach § 2 Abs. 3 Beschäftigte und Beauftragte der Endkunden
Monitoring	Automatisierte Suche nach Angeboten und Inhalten, die die Marken des Kunden missbrauchen; Erfassung, Bewertung (auch KI-gestützt) und Dokumentation der Treffer	Domain- und Registrierungsdaten (z. B. WHOIS, Zertifikatsdaten), Inhalte und Screenshots verdächtiger Websites, öffentlich abrufbare Profildaten verdächtiger Social-Media- und Business-Netzwerk-Profile (z. B. Name, Profilbild, Jobtitel, Profil-URL), Daten zu Werbeanzeigen und Werbetreibenden, Kontaktangaben auf beanstandeten Seiten	Inhaber, Betreiber und Kontaktpersonen verdächtiger Angebote; Personen, die in überwachten Inhalten vorkommen; Beschäftigte des Kunden, soweit deren öffentliche Profile zur Abgrenzung echter von gefälschten Profilen herangezogen werden
Takedown	Beweissicherung, Ermittlung der zuständigen Anbieter, Versand von Meldungen und Beschwerden im Namen des Kunden, Nachfassung, Erfolgskontrolle, Dokumentation	Falldaten (URLs, Screenshots, Seitenquelltext, technische Header, Zeitstempel), Registrierungsdaten, Korrespondenz mit Anbietern einschließlich Abuse-Kontaktadressen, Angaben des Kunden zum Fall und zu seinen Schutzrechten	Wie Monitoring; zusätzlich Beschäftigte der angeschriebenen Anbieter sowie die meldenden Personen beim Kunden
Programmierschnittstellen	Zugriff des Kunden auf die Leistungen über API, Webhooks und Integrationen	Zugangskennungen, Protokolldaten der Zugriffe, übermittelte Inhalte wie oben	Beschäftigte des Kunden; Personen nach den Zeilen oben

Besondere Kategorien personenbezogener Daten: werden nicht gezielt verarbeitet; siehe § 11 Abs. 2.

Anlage 2 – Technische und organisatorische Maßnahmen

Die Maßnahmen sind nach den Schutzzielen des Art. 32 DSGVO gegliedert.

1. Vertraulichkeit

Zutrittskontrolle

- Betrieb der Plattform, der Datenbanken und des Objektspeichers ausschließlich in Rechenzentren der Hetzner Online GmbH in Deutschland, die nach ISO/IEC 27001 zertifiziert sind und über eine physische Zutrittskontrolle verfügen.
- nebtly betreibt keine eigenen Serverräume. Arbeitsplatzrechner, auf denen Falldaten bearbeitet werden, sind mit Festplattenverschlüsselung und Bildschirmsperre geschützt.

Zugangskontrolle

- Persönliche Nutzerkonten für Plattform, Infrastruktur und Drittdienste.

- Passwörter werden ausschließlich als gesalzene Hashwerte gespeichert.
- Zwei-Faktor-Authentifizierung für administrative Zugänge zu Infrastruktur und Drittdiensten; für Plattformnutzer verfügbar. Anmeldung alternativ über Single Sign-on.
- Schutz der Anmelde- und Registrierungsvorgänge vor automatisierten Angriffen.
- Zugriff auf Programmierschnittstellen nur mit Zugangstoken; Token sind widerrufbar.

Zugriffskontrolle

- Rollen- und Berechtigungskonzept nach dem Prinzip der geringsten Rechte.
- Logische Trennung der Daten verschiedener Kunden; Nutzer sehen nur die Daten ihrer eigenen Organisation.
- Entzug von Zugängen bei Ausscheiden oder Rollenwechsel von Beschäftigten.

Trennungskontrolle

- Verarbeitung der Daten nur zu dem Zweck, zu dem sie erhoben wurden; Mandantentrennung in der Plattform.

2. Integrität

Weitergabekontrolle

- Verschlüsselung aller Verbindungen zur Plattform und zu den Programmierschnittstellen nach dem Stand der Technik (TLS).
- Beanstandete Domains werden in ausgehenden Meldungen entschärft dargestellt und nicht als anklickbare Links versandt.
- Meldungen an Dritte werden auf die für den jeweiligen Empfänger erforderlichen Angaben beschränkt.

Eingabekontrolle

- Protokollierung sicherheitsrelevanter Ereignisse und von Änderungen an Falldaten.
- Erfolgsnachweise werden mit Zeitstempel und Herkunftsangabe dokumentiert.

3. Verfügbarkeit und Belastbarkeit

- Regelmäßige Datensicherungen.
- Laufende Überwachung von Fehlern und Störungen der Plattform.
- Schutz vor automatisierten und missbräuchlichen Zugriffen.
- Ersatzmeldeweg per E-Mail bei Nichtverfügbarkeit der Plattform.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Auswahl der Unterauftragsverarbeiter unter Berücksichtigung ihrer Sicherheitsmaßnahmen; Abschluss von Verträgen nach Art. 28 DSGVO und, soweit erforderlich, von Standardvertragsklauseln.
- Einsatz von KI-Diensten nur auf Grundlage geschäftlicher Verträge mit Auftragsverarbeitungsvereinbarung und ohne Nutzung der Daten zum Modelltraining.
- Verpflichtung aller Beschäftigten auf Vertraulichkeit und regelmäßige Sensibilisierung für Datenschutz und Informationssicherheit.
- Regelmäßige Aktualisierung der eingesetzten Software und ihrer Abhängigkeiten.
- Überprüfung dieser Maßnahmen mindestens jährlich sowie anlassbezogen.
- Verfahren zur Erkennung, Bewertung und Meldung von Datenschutzverletzungen nach § 9.

Anlage 3 – Unterauftragsverarbeiter

Die jeweils aktuelle Liste der Unterauftragsverarbeiter mit Sitz, Leistung, Verarbeitungsort und Übermittlungsgrundlage ist unter nebty-id.com/de/unterauftragsverarbeiter/ abrufbar und Bestandteil dieses AVV. Änderungen erfolgen nach § 6.

nebty GmbH · c/o BASE Coworking, Blütenstraße 15, 80799 München · info@nebty-id.com

Unterauftragsverarbeiter

Anlage 3 zum Auftragsverarbeitungsvertrag der nebty GmbH

Stand: Oktober 2026

Die nebty GmbH setzt zur Erbringung ihrer Leistungen die folgenden Unterauftragsverarbeiter ein. Die Plattform, die Datenbank und die Ablage der Beweismittel werden in Deutschland betrieben. Die übrigen Dienstleister verarbeiten Daten nur für den jeweils genannten Zweck.

Über geplante Änderungen informieren wir mindestens 30 Tage im Voraus (§ 6 AVV). Wenn Sie als Kunde ohne eigenes Kundenkonto oder zusätzlich an eine weitere Adresse informiert werden möchten, schreiben Sie an info@nebty-id.com.

Für alle Leistungen

Unternehmen	Sitz	Leistung	Verarbeitungsort	Übermittlungsgrundlage
Hetzner Online GmbH	Gunzenhausen, Deutschland	Betrieb der Plattform, Datenbank, Objektspeicher für Screenshots und Beweismittel	Deutschland	– (keine Drittlandübermittlung)
Functional Software, Inc. (Sentry)	San Francisco, USA	Fehler- und Betriebsüberwachung der Plattform	Speicherung in der EU; Zugriff aus den USA möglich	EU-U.S. Data Privacy Framework; Standardvertragsklauseln
Twilio Inc. (SendGrid)	San Francisco, USA	Versand von E-Mails: Benachrichtigungen, Systemnachrichten und Takedown-Meldungen	USA	EU-U.S. Data Privacy Framework; Standardvertragsklauseln
Google Cloud EMEA Limited	Dublin, Irland	Google Workspace: geschäftliche Postfächer einschließlich der Korrespondenz mit Anbietern im Takedown; Anmeldung über Google	EU; Weiterverarbeitung in den USA	Für Weiterübermittlungen an Google LLC: EU-U.S. Data Privacy Framework; Standardvertragsklauseln
Cloudflare, Inc.	San Francisco, USA	Schutz vor automatisierten und missbräuchlichen Zugriffen; Hosting der Website; Betrieb des nebty-MCP-Servers und weiterer serverloser Funktionen (Cloudflare Pages und Workers)	weltweites Netzwerk, USA	EU-U.S. Data Privacy Framework; Standardvertragsklauseln

Zusätzlich beim Takedown

Unternehmen	Sitz	Leistung	Verarbeitungsort	Übermittlungsgrundlage
Anthropic Ireland, Limited	Dublin, Irland	KI-gestützte Bearbeitung von Takedown-Fällen	USA	Standardvertragsklauseln

Zusätzlich beim Monitoring

Unternehmen	Sitz	Leistung	Verarbeitungsort	Übermittlungsgrundlage
OpenAI Ireland Limited	Dublin, Irland	KI-gestützte Bewertung von Treffern	USA	Standardvertragsklauseln

Unternehmen	Sitz	Leistung	Verarbeitungsort	Übermittlungsgrundlage
OpenRouter, Inc.	USA	Zugang zu KI-Modellen für die Bewertung von Treffern	USA	Standardvertragsklauseln
Bright Data Ltd.	Netanja, Israel	Abruf öffentlich zugänglicher Webinhalte	Israel	Angemessenheitsbeschluss (Israel)
Oxylabs, UAB	Vilnius, Litauen	Proxy-Infrastruktur für den Abruf öffentlich zugänglicher Webinhalte	EU	– (keine Drittlandübermittlung)
VostokInc SAS (ScrapingBee)	Paris, Frankreich	Abruf und Darstellung von Webseiten, Screenshots	Frankreich	– (keine Drittlandübermittlung)

Keine Unterauftragsverarbeiter

Nicht in dieser Liste stehen Stellen, die Daten in eigener Verantwortung verarbeiten:

- **Empfänger von Takedown-Meldungen** wie Registrare, Hosting-Anbieter, Plattformbetreiber, Suchmaschinen und Betreiber von Sicherheits-Blacklists (§ 3 Abs. 3 und § 7 Abs. 4 AVV).
- **Datenquellen**, die nebyty abfragt, etwa öffentliche Register, Zertifikatsprotokolle und die Werbebibliotheken von Plattformen.
- **Zahlungsdienstleister**, die im Rahmen der Abrechnung tätig werden; die Abrechnung ist eine Verarbeitung von nebyty in eigener Verantwortung (§ 3 Abs. 1 AVV).
- **Dienste des Kunden**, an die der Kunde Benachrichtigungen weiterleitet, etwa per Webhook oder an Messenger-Kanäle (§ 11 Abs. 4 AVV).