Vertrag über die Auftragsverarbeitung gemäß Art. 28 DSGVO

Stand der Vorlage: 27. April 2026 (das Vertragsdatum ergibt sich aus dem Tag der Buchung im TrustBoost-Kundenportal)
Version: 1.4
Gilt für: TrustBoost (Service der Neu-Protec)
Zielgruppe: Unternehmer im Sinne des § 14 BGB (B2B)

Zwischen

dem Kunden (im Folgenden „Verantwortlicher")

neu-protec Mediendesign
Hamburger Str. 43
40221 Düsseldorf
Deutschland
Vertreten durch
Thomas Perke

Kontakt

Telefon: 0156 78 281 339
E-Mail: info@cleancalc.de

wird der folgende Vertrag zur Auftragsverarbeitung (im Folgenden „AVV") gemäß Art. 28 DSGVO geschlossen.

---

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Gegenstand des Auftrags ist die Bereitstellung und der Betrieb des Online-Dienstes **TrustBoost** zur Sammlung, Filterung, Auswertung und Darstellung von Kundenbewertungen sowie zugehörige technische Dienstleistungen (Hosting, Wartung, Support).

1.2 Dauer

Der Auftrag wird auf unbestimmte Zeit geschlossen und ist an die Laufzeit des Hauptvertrags (TrustBoost-Abonnement) gekoppelt. Er endet automatisch mit Beendigung des Hauptvertrags.

2. Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der Verarbeitung

- Betrieb der Bewertungs- und Feedback-Formulare des Verantwortlichen
- Speicherung und Anzeige von Sterne-Bewertungen
- Weiterleitung zufriedener Kunden zu Google
- Erfassung und Bereitstellung von internem Feedback unzufriedener Kunden
- Auslieferung des Bewertungssiegels (iFrame / JavaScript)
- Bereitstellung von Druckmaterialien mit personalisiertem QR-Code
- Versand transaktionaler E-Mails (z. B. Onboarding, Benachrichtigungen)

2.2 Art der personenbezogenen Daten

- **Stammdaten:** Name, E-Mail-Adresse, Firma, Anschrift (des Verantwortlichen und seiner Mitarbeiter:innen)
- **Bewertungsdaten:** Sterne-Bewertung, Freitext-Feedback, Datum/Uhrzeit
- **Optionale Kontaktdaten der Endkunden:** Name, E-Mail, Telefonnummer (sofern im Feedback-Formular eingegeben)
- **Technische Daten:** IP-Adresse (gekürzt), User-Agent, Zeitstempel, Referrer
- **Vertrags- und Abrechnungsdaten:** Plan, Buchungszeitraum, Zahlstatus

2.3 Kategorien betroffener Personen

- Verantwortlicher und seine Mitarbeiter:innen / Bevollmächtigten
- Endkunden des Verantwortlichen, die das Bewertungs- oder Feedback-Formular nutzen
- Webseiten-Besucher:innen, die das Bewertungssiegel sehen

2.4 Besondere Datenkategorien

Eine Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO ist nicht vorgesehen. Der Verantwortliche stellt durch Gestaltung seiner Formulare sicher, dass keine solchen Daten erhoben werden.

---

3. Rechte und Pflichten des Verantwortlichen

3.1 Für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Verantwortliche zuständig.

3.2 Der Verantwortliche erteilt alle Aufträge, Teilaufträge und Weisungen grundsätzlich in Textform. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

3.3 Der Verantwortliche ist berechtigt, sich vor Beginn und während der Laufzeit des Auftrags von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen (TOMs) beim Auftragsverarbeiter zu überzeugen.

3.4 Der Verantwortliche benennt für vertragliche Fragen folgende Kontaktperson: gemäß Angaben im Kundenportal (E-Mail-Adresse des Account-Inhabers).

---

4. Allgemeine Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Verantwortlichen, es sei denn, er ist gesetzlich zu einer anderen Verarbeitung verpflichtet. In einem solchen Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern dies nicht gesetzlich verboten ist.

Der Auftragsverarbeiter sichert insbesondere zu:

a) Bestellung eines Datenschutzbeauftragten, sofern gesetzlich vorgeschrieben. Da der Auftragsverarbeiter aktuell nicht zur Bestellung eines Datenschutzbeauftragten gemäß § 38 BDSG verpflichtet ist, ist kein DSB benannt. Datenschutzanfragen werden zentral bearbeitet – Kontakt: datenschutz@neu-protec.de. Sobald eine Bestellpflicht entsteht, wird ein DSB benannt und der Verantwortliche über die Kontaktdaten informiert.

b) Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO. Der Auftragsverarbeiter setzt bei der Durchführung nur Beschäftigte ein, die zur Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten datenschutzrechtlichen Bestimmungen vertraut gemacht worden sind.

c) Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO (siehe **Anlage 1**).

d) Unverzügliche Information des Verantwortlichen über Kontrollen oder Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

e) Unverzügliche Mitteilung an den Verantwortlichen, falls der Auftragsverarbeiter der Auffassung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt.

f) Unterstützung des Verantwortlichen bei der Wahrung der Betroffenenrechte (Art. 12–22 DSGVO), bei Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) sowie bei der Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33, 34 DSGVO).

g) Löschung oder Rückgabe sämtlicher Daten nach Beendigung des Auftrags gemäß Ziffer 10.

---

5. Subunternehmerverhältnisse (weitere Auftragsverarbeiter)

5.1 Der Verantwortliche willigt allgemein in den Einsatz weiterer Auftragsverarbeiter (Subunternehmer) ein. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Subunternehmer sind in **Anlage 2** abschließend aufgeführt und vom Verantwortlichen genehmigt.

5.2 Der Auftragsverarbeiter informiert den Verantwortlichen vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter. Der Verantwortliche kann dieser Änderung innerhalb von **30 Tagen** in Textform widersprechen, wenn berechtigte Gründe vorliegen.

5.3 Der Auftragsverarbeiter verpflichtet jeden Subunternehmer durch einen Vertrag, in dem im Wesentlichen die gleichen Datenschutzpflichten auferlegt werden wie in dieser Vereinbarung.

5.4 Findet eine Übermittlung in ein Drittland statt, stellt der Auftragsverarbeiter ein angemessenes Datenschutzniveau sicher. Dies erfolgt vorrangig auf Grundlage eines Angemessenheitsbeschlusses (z. B. EU-US Data Privacy Framework für zertifizierte US-Empfänger) und – sofern ein solcher nicht greift – auf Grundlage der EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914) im jeweils einschlägigen Modul (Modul 2 oder 3, je nach Konstellation) zuzüglich erforderlicher ergänzender Maßnahmen (Transfer Impact Assessment, TOMs).

---

6. Technische und organisatorische Maßnahmen (TOMs)

Die zum Zeitpunkt des Vertragsschlusses getroffenen TOMs ergeben sich aus **Anlage 1** und sind ausreichend i. S. d. Art. 32 DSGVO. Sie können während der Vertragsdauer der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen jedoch das vereinbarte Schutzniveau nicht unterschreiten.

---

7. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragsverarbeiter darf die im Auftrag verarbeiteten Daten nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter.

---

8. Kontrollrechte des Verantwortlichen

8.1 Der Verantwortliche überzeugt sich vor Beginn und während der Vertragslaufzeit von der Einhaltung der TOMs. Hierzu kann er Auskünfte einholen oder vor Ort eine Inspektion mit angemessener Vorlaufzeit (mindestens 14 Tage) während der üblichen Geschäftszeiten ohne Störung des Betriebsablaufs vornehmen.

8.2 Der Auftragsverarbeiter kann die Einhaltung auch durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. ISO 27001, BSI-Grundschutz, Penetrationstests) nachweisen.

8.3 Die Kosten einer vom Verantwortlichen beauftragten Vor-Ort-Prüfung trägt der Verantwortliche, sofern keine wesentlichen Mängel festgestellt werden.

---

9. Mitteilung bei Verstößen des Auftragsverarbeiters

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von **72 Stunden** nach Kenntniserlangung, über alle Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO. Die Mitteilung enthält mindestens die in Art. 33 Abs. 3 DSGVO geforderten Angaben.

---

10. Beendigung des Auftrags

10.1 Nach Abschluss der Auftragsverarbeitung – spätestens **30 Tage** nach Beendigung des Hauptvertrags – hat der Auftragsverarbeiter sämtliche in seinem Besitz befindliche personenbezogene Daten nach Wahl des Verantwortlichen entweder zurückzugeben oder zu löschen, einschließlich aller Kopien, sofern nicht eine gesetzliche Aufbewahrungspflicht besteht.

10.2 Backup-Kopien werden im üblichen Backup-Zyklus rollierend nach **30 Tagen** automatisch überschrieben bzw. gelöscht (siehe Anlage 1, Ziffer 3). Eine sofortige Löschung aus laufenden Backups ist aus technischen Gründen nicht möglich; der Auftragsverarbeiter stellt sicher, dass die Daten in dieser Zeit ausschließlich verschlüsselt vorgehalten und nicht weiterverarbeitet werden.

10.3 Die Dokumentation, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dient, wird durch den Auftragsverarbeiter entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt.

---

11. Haftung

Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Innenverhältnis haften die Parteien jeweils im Verhältnis ihres Verantwortungsanteils am Schaden.

---

12. Schlussbestimmungen

12.1 Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt.

12.2 Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Sofern der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist, ist ausschließlicher Gerichtsstand der Sitz des Auftragsverarbeiters. Im Übrigen gelten die gesetzlichen Gerichtsstände.

12.3 Im Falle von Widersprüchen zwischen dieser Vereinbarung und sonstigen Vereinbarungen der Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieser Vereinbarung in Bezug auf die Auftragsverarbeitung vor.

Anlage 1 – Technische und organisatorische Maßnahmen (TOMs) gemäß Art. 32 DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle (physisch)

- Hosting in zertifizierten Rechenzentren in Deutschland (ISO 27001)
- Zutritt nur für autorisiertes Personal mit Ausweiskontrolle
- Videoüberwachung, Alarmanlagen, 24/7 Sicherheitsdienst
- Protokollierung aller Zutritte

1.2 Zugangskontrolle (System)

- Persönliche Benutzerkonten, keine Sammelaccounts
- Starke Passwörter (mind. 12 Zeichen, Komplexität erzwungen)
- Zwei-Faktor-Authentifizierung (2FA) für administrative Zugänge verpflichtend
- Automatische Sperrung nach Fehlversuchen
- VPN-Pflicht für interne Administrationszugänge
- Rollenbasiertes Berechtigungskonzept (Need-to-know)

1.3 Zugriffskontrolle (Daten)

- Differenzierte Berechtigungen pro Rolle (Admin / Support / Kunde)
- Zugriffsprotokollierung
- Trennung von Produktiv-, Test- und Entwicklungssystemen
- Verschlüsselung von Festplatten der Endgeräte (Full Disk Encryption)

1.4 Trennungskontrolle

- Mandantenfähige Datenbankarchitektur
- Logische Trennung der Kundendaten durch Mandanten-IDs
- Getrennte Verarbeitung für unterschiedliche Zwecke (Bewertung, Abrechnung, Support)

1.5 Pseudonymisierung

- IP-Adressen werden gekürzt gespeichert
- Bewertungs-IDs als Zufalls-Token, keine Rückschlüsse auf Personen aus URL

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Verschlüsselte Übertragung (TLS 1.2+ / HTTPS) zwischen Browser, Server und Drittdiensten
- Datenexporte ausschließlich über authentifizierte Kanäle
- E-Mail-Versand über TLS-fähige SMTP-Server

2.2 Eingabekontrolle

- Logging aller administrativen Änderungen mit User-ID und Zeitstempel
- Versionierung kritischer Konfigurationen
- Audit-Trails für Backend-Aktionen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Tägliche automatisierte Backups, verschlüsselt gespeichert
- Aufbewahrung Backups: 30 Tage rollierend
- Monitoring (24/7) mit automatischen Alarmen
- DDoS-Schutz auf Infrastrukturebene
- Notfall- und Wiederanlaufplan (Disaster Recovery)
- USV und redundante Stromversorgung im Rechenzentrum
- RAID-Speicher und georedundante Backup-Standorte (innerhalb der EU)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Datenschutz-Management dokumentiert
- Regelmäßige Schulungen der Mitarbeiter:innen (mind. jährlich)
- Verpflichtung aller Beschäftigten auf Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO)
- Incident-Response-Prozess dokumentiert
- Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) wird geführt
- Jährliche Überprüfung der TOMs
- Software-Updates und Sicherheits-Patches werden zeitnah eingespielt
- Regelmäßige Penetrationstests / Vulnerability Scans

5. Auftragskontrolle

- Schriftliche AV-Verträge mit allen Subunternehmern
- Sorgfältige Auswahl von Subunternehmern unter Datenschutzaspekten
- Regelmäßige Kontrolle der Subunternehmer

Anlage 2 – Liste der Subunternehmer (Stand: 27.04.2026)

Subunternehmer	Sitz	Zweck	Datenkategorien	Garantien
[Hosting-Provider einsetzen, z. B. Hetzner Online GmbH]	Deutschland	Server-Hosting, Rechenzentrum	Alle im Rahmen des Dienstes verarbeiteten Daten	AVV nach Art. 28 DSGVO, ISO 27001
Stripe Payments Europe, Ltd.	Irland (EU); konzerninterne Weiterleitung in die USA (Stripe, Inc.) möglich	Zahlungsabwicklung	Name, E-Mail, Adresse, Zahlungsdaten	AVV, EU-Standardvertragsklauseln, PCI-DSS Level 1
Google Ireland Ltd. (Google Places API)	Irland (EU)	Abruf öffentlicher Bewertungsdaten	Geschäfts-ID des Verantwortlichen, keine Endkundendaten	Google Cloud DPA, EU-SCC
[Transaktionaler E-Mail-Provider, z. B. Brevo SAS / Mailjet]	Frankreich (EU)	Versand transaktionaler E-Mails	E-Mail-Adresse, Name	AVV, EU-Hosting
[Backup-Provider, sofern abweichend]	EU	Verschlüsselte Backup-Speicherung	Verschlüsselte Backup-Daten	AVV, EU-Hosting

Hinweis: Diese Liste wird laufend gepflegt. Änderungen werden gemäß Ziffer 5.2 dieses AVV mitgeteilt.

Dokument-Version 1.0 – Stand 27.04.2026 – Neu-Protec