Auftragsverarbeitungsvertrag (AVV)

nach Art. 28 DSGVO

zwischen

inci solutions GmbH
Gehlengraben 2
22415 Hamburg, Deutschland
E-Mail: info@incisolutions.com
(im Folgenden "**Auftragsverarbeiter**")

und

dem jeweiligen Nutzer/Kunden der Webanwendung „incisolutions-lab“
(im Folgenden: "**Auftraggeber**")

§1 GEGENSTAND UND DAUER DES AUFTRAGS

(1) Dieser Vertrag regelt die Rechte und Pflichten der Vertragsparteien im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Auftraggebers gemäß Art. 28 DSGVO.

(2) Die Verarbeitung erfolgt im Rahmen der Nutzung der webbasierten Anwendung „incisolutions-lab“ durch den Auftraggeber. Der AVV tritt mit Beginn der Nutzung in Kraft und gilt für die Dauer der Nutzung sowie für weitere drei Monate zur Gewährleistung der ordnungsgemäßen Datenrückgabe oder -löschung, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

(3) Der Vertragsschluss über die Auftragsverarbeitung erfolgt elektronisch im Rahmen der Beauftragung eines Benutzerzugangs zur Webanwendung durch den Auftraggeber. Mit der Zuteilung des Zugangs und der anschließenden Nutzung der Webanwendung gilt dieser Vertrag als rechtsverbindlich geschlossen.

§2 ZWECK DER VERARBEITUNG

(1) Die Verarbeitung erfolgt ausschließlich zur technischen Bereitstellung, dem Betrieb sowie der Nutzung der Webanwendung „incisolutions-lab“ durch den Auftraggeber.

(2) Die Zwecke der Verarbeitung umfassen:
- Verwaltung und Bearbeitung geschäftsrelevanter Daten zur Produktentwicklung kosmetischer Erzeugnisse
- Benutzerverwaltung, Rechte- und Rollenzuweisung
- Hosting und Datenspeicherung über einen externen Hostinganbieter (STRATO GmbH, Deutschland)
- Erstellung regelmäßiger Backups zur Datensicherung
- Technische Fehlerprotokollierung zur Diagnose und Sicherstellung des stabilen Betriebs
- Unterstützung bei technischen Fragen (optional)

§3 ART DER VERARBEITETEN DATEN UND BETROFFENE PERSONEN

(1) Betroffene Personengruppen:
- Auftraggeber selbst (z. B. Ansprechpartner des Unternehmens)
- Nutzer der Webanwendung (z. B. Mitarbeitende des Auftraggebers)

- Geschäftspartner des Auftraggebers (z. B. Kunden, Lieferanten), deren Daten durch die Nutzer eingegeben werden

(2) Kategorien personenbezogener Daten:
- Benutzerdaten: Vor- und Nachname, E-Mail-Adresse, Benutzername, IP-Adresse, Passwort (verschlüsselt)
- Kontaktdaten: Name, Anschrift, E-Mail-Adresse, Telefonnummer von Geschäftspartnern
- Metadaten: Benutzerkennung, Zeitstempel bei Erstellung oder Änderung von Datensätzen
- Kommunikationsdaten: E-Mail-Adresse für optional aktivierte Systembenachrichtigungen
- Fehlerprotokolldaten: Pseudonymisierte Mandanten- oder Unternehmenskennungen im Rahmen technischer Fehlerprotokollierung
- Medieninhalte: Firmenlogo (optional)

Hinweis: Die Verantwortung für die rechtmäßige Verarbeitung und Eingabe der Daten liegt beim Auftraggeber.

§4 PFLICHTEN DES AUFTRAGSVERARBEITERS

Der Auftragsverarbeiter verpflichtet sich:

- personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers zu verarbeiten
- keine eigenständige Nutzung oder Weitergabe der Daten vorzunehmen
- ausschließlich zur Vertraulichkeit verpflichtetes Personal einzusetzen
- geeignete technische und organisatorische Maßnahmen (TOMs) umzusetzen und auf dem aktuellen Stand zu halten
- den Auftraggeber unverzüglich über Datenschutzverletzungen zu informieren
- nur vertraglich geregelte Subunternehmer einzusetzen
- den Auftraggeber bei der Wahrnehmung seiner datenschutzrechtlichen Pflichten (Betroffenenrechte, Datenschutz-Folgenabschätzungen, Meldungen) zu unterstützen
- Daten nach Vertragsende entsprechend §10 zu löschen oder zurückzugeben

§5 WEISUNGSRECHT

(1) Der Auftragsverarbeiter handelt ausschließlich auf dokumentierte Weisung des Auftraggebers.

(2) Weisungen erfolgen grundsätzlich in Textform, vorzugsweise per E-Mail. In Ausnahmefällen mündlich erteilte Weisungen sind innerhalb von drei Werktagen schriftlich zu bestätigen.

§6 TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOM)

Die getroffenen TOMs umfassen u. a.:

- Zugriffskontrolle: Rollenbasiertes Berechtigungssystem, Passwortverschlüsselung mit bcrypt
- Netzwerk- und Transportsicherheit: TLS/SSL-Verschlüsselung, IP-Whitelisting, Firewall
- Angriffserkennung: Einsatz von Software zur automatisierten Erkennung und Abwehr verdächtiger Login-Versuche
- Speicherung: Datenverarbeitung ausschließlich auf Servern innerhalb der EU (Deutschland, STRATO GmbH)
- Backups: Regelmäßige, verschlüsselte Backups mit Löschung spätestens nach 3 Monaten
- Vertraulichkeit: Schriftliche Vertraulichkeitsvereinbarungen mit allen Mitarbeitenden mit Datenzugang
- Datenzugriff: Kein Zugriff auf Kundendaten ohne ausdrückliche Anforderung durch den Auftraggeber im Rahmen eines Supportfalls oder bei gesetzlicher Verpflichtung

§7 RECHTE UND PFLICHTEN DES AUFTRAGGEBERS

(1) Der Auftraggeber bleibt datenschutzrechtlich Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO und Eigentümer der verarbeiteten personenbezogenen Daten.

(2) Der Auftraggeber ist verantwortlich für:
- die rechtmäßige Verarbeitung der personenbezogenen Daten in der Webanwendung
- die Erfüllung der Informationspflichten gegenüber betroffenen Personen nach Art. 13 und 14 DSGVO

§8 SUBUNTERNEHMER

(1) Für das Hosting wird die STRATO GmbH, Otto-Ostrowski-Straße 7, 10249 Berlin eingesetzt. Ein AVV gemäß Art. 28 DSGVO ist abgeschlossen.

(2) Weitere Subunternehmer dürfen nur mit vorheriger schriftlicher Zustimmung des Auftraggebers eingesetzt werden.

(3) Eine Verarbeitung personenbezogener Daten in einem Drittland findet nicht statt.

§9 KONTROLLRECHTE DES AUFTRAGGEBERS

(1) Der Auftraggeber ist berechtigt, die Einhaltung dieses AVV durch folgende Maßnahmen zu prüfen:
- Einsicht in die TOMs
- Anforderung geeigneter Nachweise
- Durchführung eines Audits nach vorheriger Ankündigung (vor Ort oder remote)

(2) Die Kontrollmaßnahmen erfolgen mit angemessener Vorlaufzeit, in zumutbarem Umfang und unter Wahrung der Vertraulichkeit.

§10 LÖSCHUNG UND RÜCKGABE VON DATEN

(1) Der Auftraggeber kann während der Laufzeit Daten eigenständig exportieren oder löschen.

(2) Nach Vertragsende erfolgt die vollständige Löschung aller personenbezogenen Daten innerhalb von 12 Monaten – einschließlich der Backups (nach spätestens 3 Monaten), sofern keine gesetzlichen Aufbewahrungspflichten bestehen.

(3) Auf schriftliche Anfrage stellt der Auftragsverarbeiter dem Auftraggeber vorab einen Export der Daten zur Verfügung.

§11 VERTRAULICHKEIT

(1) Alle Mitarbeitenden des Auftragsverarbeiters sind schriftlich zur Vertraulichkeit verpflichtet.

(2) Diese Pflicht erstreckt sich auch auf nicht-personenbezogene Daten wie Rezepturen, Rohstoffinformationen und Geschäftsgeheimnisse des Auftraggebers.

(3) Ein Zugriff auf gespeicherte Daten erfolgt ausschließlich bei ausdrücklicher Supportanfrage oder rechtlicher Verpflichtung.

§12 SCHLUSSBESTIMMUNGEN

(1) Ergänzende Vereinbarungen, wie SLAs oder Verfügbarkeitsgarantien, sind nicht Bestandteil dieses AVV, können jedoch separat vereinbart werden.

(2) Der AVV gilt in der jeweils aktuellen Version. Änderungen werden dem Auftraggeber rechtzeitig mitgeteilt.

(3) Bei Widersprüchen zwischen diesem AVV und sonstigen Vertragsdokumenten geht dieser AVV in datenschutzrechtlichen Belangen vor.

(4) Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftragsverarbeiters (inci solutions GmbH).

Stand: April 2025